TELEMÁTICA
REVISTA DIGITAL de las Tecnologías de la Información y las Telecomunicaciones
Revista Telemática. Vol.20 No.1, Enero-Marzo, 2021, p.27-35 ISSN 1729-3804

MECANISMO SIMPLE PARA DETECCIÓN DE POSIBLE FUGA DE INFORMACIÓN EN REDES DE DATOS

Javier Alfonso Valdés[1]

[1]Fiscalía General de la República, Avenida 1ra, No. 1801 e/ 18 y 20. Reparto Miramar, municipio Playa, La Habana, Cuba
[1]e-mail: jalfonso@fgr.gob.cu, jalfonsocu@gmail.com

RESUMEN

La fuga de información sensible es uno de los principales problemas que enfrentan las instituciones. Herramientas tradicionales como Snort o Suricata, basadas en reglas, son capaces de detectar de manera eficiente amenazas conocidas, pero son inútiles contra las APT (Amenazas Persistentes Avanzadas, por sus siglas en ingles). Las APT utilizan vulnerabilidades desconocidas y protocolos estándares con cifrado con lo cual se consigue la simulación de un comportamiento normal. En la presente investigación se propone un método simple basado en la desviación estándar de los tiempos entre arribo de flujos cuyo propósito es la detección de conexiones salientes periódicas que luego puedan ser analizadas por especialistas en búsqueda de fuga de información. Fueron identificadas conexiones periódicas sospechosas y entre éstas, una que se corresponde a un servicio mal configurado que reportaba datos de usuario, observándose efectivamente un caso de fuga de información.

PALABRAS CLAVES: fuga de información, periodicidad, tráfico de red, desviación estándar.

SIMPLE MECHANISM FOR POSSIBLE INFORMATION LEAK DETECTION ON DATA NETWORKS

ABSTRACT

The leakage of sensitive information is one of the main problems faced by institutions. Traditional rules-based tools like Snort or Suricata are able to efficiently detect known threats, but are useless against APTs (Advanced Persistent Threats). APTs use unknown vulnerabilities and standard protocols with encryption, simulating normal behavior. In this research a simple method based on the standard deviation of the times between the arrival of flows is proposed. It seeks to detect periodic outgoing connections that can be analyzed by specialists in search of information leakage. Suspicious periodic connections were identified, one of them corresponding to a poorly configured service that reported user data, effectively identifying a case of information leakage.

INDEX TERMS: information leak, periodicity, network traffic, standard deviation.

1. INTRODUCCIÓN

La fuga de información sensible a través de las redes de datos es uno de los principales riesgos que enfrentan actualmente las organizaciones [1]. Las revelaciones de Edward Snowden confirmaron la existencia de herramientas de software diseñadas para la extracción de datos de forma encubierta, haciendo pasar este tráfico como legítimo [2].

Las soluciones tradicionales basadas en reglas son capaces de detectar de manera eficiente amenazas conocidas, pero son inútiles contra las APT (Amenazas Persistentes Avanzadas). Las APT utilizan vulnerabilidades desconocidas y protocolos estándares con cifrado, simulando un comportamiento normal [3].

Una red analizada de aproximadamente 2 000 usuarios genera un promedio de 525 Gbytes de tráfico diariamente, por lo que resulta inviable su almacenamiento en disco por tiempo indefinido. Una alternativa ampliamente utilizada es el empleo de las trazas de *netflow* (flujos de red) que almacenan un resumen de las conexiones establecidas. Estas trazas usualmente se encuentran disponibles para el análisis por parte de los especialistas de seguridad informática y generan un promedio de 1 326 010 líneas diarias. La reducción del volumen total de conexiones a revisar a una cantidad manejable, haría más eficiente el trabajo de los especialistas e incrementaría su tasa de detección.

Manuscrito recibido: 2020-09-21, aceptado: 2020-12-04
Sitio web:http://revistatelematica.cujae.edu.cu/index.php/tele

Los usuarios humanos generalmente tienen una rutina de uso de Internet, pero esta tiene un período largo, mayormente de un día y con una variabilidad alta. En el caso de los programas malignos, estos períodos son menores, variando de segundos a horas. Este comportamiento periódico puede ser utilizado para detectar actividad maliciosa [4] [5]. Existen también varios servicios legítimos capaces de mostrar un comportamiento de este tipo, como los servicios de actualizaciones de programas y sistemas operativos, por lo que corresponde a un analista de seguridad discriminar los patrones legítimos de los no legítimos [6].

El objetivo del presente trabajo es presentar un método inicial simple para detectar posibles fugas de información oculta en el tráfico legítimo de una red corporativa a partir de su periodicidad. Será responsabilidad de los analistas de seguridad informática determinar si los elementos detectados corresponden con actividad maliciosa o no.

Debido al gran volumen de información que se genera en una red de computadoras, no se analiza todo el tráfico, solo las trazas de *netflow* (flujo de red) que incluyen:

- **timestamp**: Marca de tiempo de inicio del flujo.
- **IP_src**: IP origen.
- **IP_dest**: IP destino.
- **bytes_toclient**: Bytes a cliente.
- **bytes_toserver**: Bytes a destino.
- **pkts_toclient**: Paquetes a cliente.
- **pkts_toserver**: Paquetes a destino.
- **age**: Duración del flujo.

El método propuesto consiste en identificar pares de direcciones IP con tránsitos de información en sentido ascendente (subida) con el propósito de analizar sus trazas en busca de evidencias de actividad automática, dando como resultado un listado de direcciones sospechosas que deberán ser analizadas manualmente. Para identificar actividad periódica se utiliza la desviación estándar de los tiempos entre arribo de flujos de red consecutivos [7].

El algoritmo fue seleccionado debido a su facilidad de implementación y alto rendimiento, permitiendo procesar grandes volúmenes de trazas en corto tiempo con equipamiento de bajas prestaciones. Para las pruebas se dispone de una computadora portátil con procesador de cuatro núcleos a 2 GHz y 4 Gbyte de memoria RAM.

El presente artículo queda estructurado en cuatro secciones: Sección 1, introducción al tema y planteamiento de la situación problémica; Sección 2, describe el método propuesto y consideraciones de implementación para un tiempo de ejecución aceptable; Sección 3, se presentan los resultados obtenidos de aplicar el método a trazas de una red corporativa real.

2. MÉTODO PROPUESTO

La red analizada no provee servicios al exterior, por lo que la casi totalidad del tráfico corresponde con navegación web, envío de correo electrónico y resolución de nombres de dominio, mediante los protocolos DNS, SMTP, HTTPS y HTTP, prevaleciendo las descargas. Se consideran normales las trazas de flujo de red que muestran:

$$bytes_{toclient} > bytes_{toserver} \quad (1)$$

El método consta de tres pasos que se detallan a continuación:

Paso 1:
Se procesan los ficheros de trazas, eliminando las líneas que incumplan con la ecuación (1), reduciendo el total a procesar.

Paso 2:
Se ordena el resultado del **Paso 1** de menor a mayor por la marca de tiempo de inicio de los flujos [7].

Paso 3:
Una vez depurada y ordenada la información correspondiente a las trazas donde hay tráfico saliente de la red, se detecta periodicidad en los flujos, lo que es indicador de actividad automática. Para determinar periodicidad se analizan similitudes en los tiempos entre arribo de flujos sucesivos, calculando la desviación estándar de estos valores por cada par existente de direcciones IP origen y destino [7].

TELEMÁTICA
REVISTA DIGITAL de las Tecnologías de la Información y las Telecomunicaciones
Revista Telemática. Vol.20 No.1, Enero- Marzo, 2021, p.27-35 ISSN 1729-3804

Para ello se utiliza la fórmula de la desviación estándar para una muestra de población:

$$s = \sqrt{\frac{1}{(N-1)}\sum_{i=1}^{N}(x_i - \mu)^2} \quad (2).$$

Debido a que una desviación estándar baja de los tiempos entre arribo de los flujos indica que estos se encuentran cercanos, la utilizamos para definir y detectar periodicidad en el tráfico.

Parámetros:
Se consideran periódicas una serie de conexiones si:

- La cantidad de flujos detectados es mayor que un número ***n***.
- El tiempo transcurrido entre el primer y último flujo detectado es mayor que un lapso ***t***.
- La desviación estándar calculada es menor que un límite ***s***.

Para la implementación se emplea el lenguaje de programación Java debido a que se busca una solución multiplataforma, sencilla de ejecutar en diferentes sistemas operativos y arquitecturas de computadora. Fue utilizada la plataforma de desarrollo OpenJDK versión 11.0.8

Teniendo en cuenta que el cálculo de la desviación estándar requiere de operaciones como división y raíz cuadrada, lo que introduce valores con punto flotante cuya precisión es importante para el resultado del algoritmo, se utiliza la biblioteca ***Apache Commons Math*** [8], que implementa diversos algoritmos estadísticos. Además, se utilizan las funciones de la biblioteca que aplican los métodos de cálculo rápido, permitiendo obtener el resultado agregando datos en vez de recorrer una lista una vez obtenidos todos los valores, reduciendo el coste computacional de la solución.

Uno de los principales cuellos de botella identificados radica en la lectura de los ficheros de trazas, ya que es necesario obtener todas las marcas de tiempo por cada par de direcciones IP presentes. Esto requiere de múltiples lecturas de disco que ralentizan la aplicación. Fueron utilizadas estructuras de datos que permiten obtener la información necesaria en una sola lectura de los ficheros de entrada.

3. RESULTADOS

La selección de los parámetros para la ejecución del método afecta el resultado, ya que este tipo de algoritmos es sensible a la ventana de tiempo seleccionada y deberán seleccionarse en dependencia del tipo de comportamiento que se espera encontrar. Para el experimento fueron utilizados los parámetros explicados anteriormente, asignándose a los mismos los siguientes valores:

- La cantidad de flujos detectados es mayor que 10.
- El tiempo transcurrido entre el primer y último flujo detectado es mayor que un lapso de 10 minutos.
- La desviación estándar calculada es menor que un límite de 4 segundos.

El método fue ejecutado con trazas pertenecientes a cinco días laborables, con un total de 20856064 líneas, de las cuales solo 5812108 fueron analizadas al cumplir con la ecuación (1), generando 172173 pares de direcciones IP.

Los parámetros seleccionados influyen en la cantidad de resultados identificados, en este caso, se obtuvo una lista de 10 pares de direcciones IP. De estas analizaremos casos de muestra que reflejan diferentes situaciones con las que puede encontrarse un analista de seguridad informática. Como primer paso para identificar direcciones maliciosas fue utilizado el servicio AbuseIPDB.

AbuseIPDB [9], disponible en **HTTP://ABUSEIPDB.COM**, es un proyecto dedicado a combatir la proliferación de ataques y actividad abusiva en Internet. Provee una lista negra central de direcciones IP que han sido asociadas a actividad maliciosa. Los usuarios pueden reportar direcciones que hayan detectado como maliciosas o consultar el registro de una dirección.

Para evaluar la fiabilidad del método es necesario considerar falsos positivos y falsos negativos. Debido a que no se conoce con seguridad como lucen los datos, se realizan representaciones gráficas de las conexiones con el objetivo de identificar patrones periódicos. Las representaciones gráficas muestran los ***timestamp*** (Eje Y, Tiempo) con respecto

al número del flujo correspondiente (Eje X, Flujos). Mientras más regular sean los tiempos entre arribo, más similar a una recta será el resultado.

Para apoyar en el análisis se calcula la línea de tendencia de los ***timestamp***, la gráfica de una conexión periódica será similar a una recta y la distancia entre cada punto y su tendencia será baja. Aquellas direcciones donde el número de conexiones es alto y frecuente, tiene tiempos entre arribo pequeños, por lo que el método la detectará al ser la desviación estándar baja, pero no necesariamente se corresponde con una conexión periódica, si se separa de la recta de tendencia, se considera un falso positivo.

Caso de muestra: IP 178.250.6.59

La dirección IP 178.250.6.59 (Figura 1) está registrada a un centro de datos para hospedaje de servicios ubicado en Francia. No se encuentra en la base de datos de AbuseIPDB.

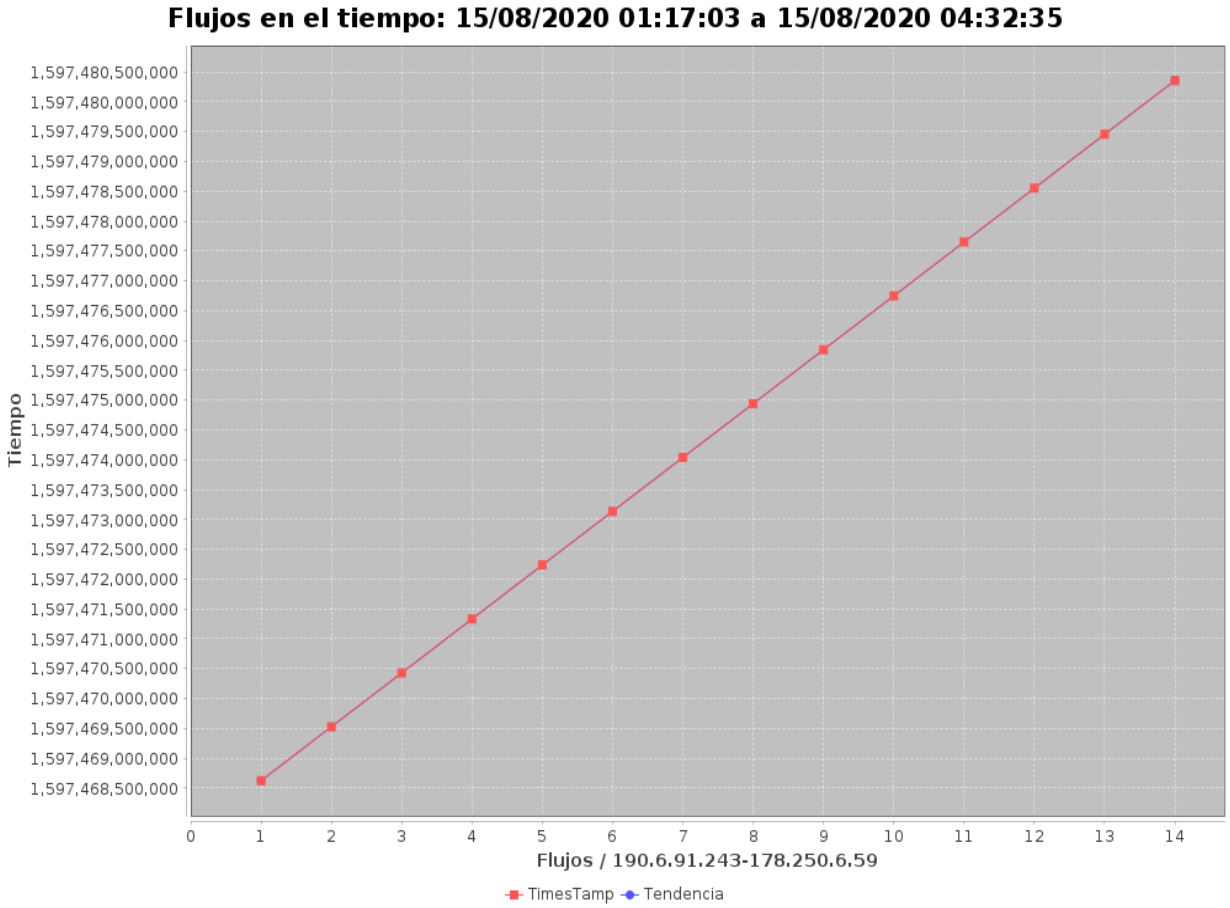

Figura 1: Conexiones IP 178.250.6.59.

Caso de muestra: IP 141.218.143.78

Esta dirección IP (Figura 2) se encuentra registrada como perteneciente a la Universidad de Michigan Oeste, con nombre de dominio *yakko.cs.wmich.edu,* ha sido reportada 14 veces en el servicio de AbuseIPDB.

TELEMÁTICA
REVISTA DIGITAL de las Tecnologías de la Información y las Telecomunicaciones
Revista Telemática. Vol.20 No.1, Enero- Marzo, 2021, p.27-35 ISSN 1729-3804

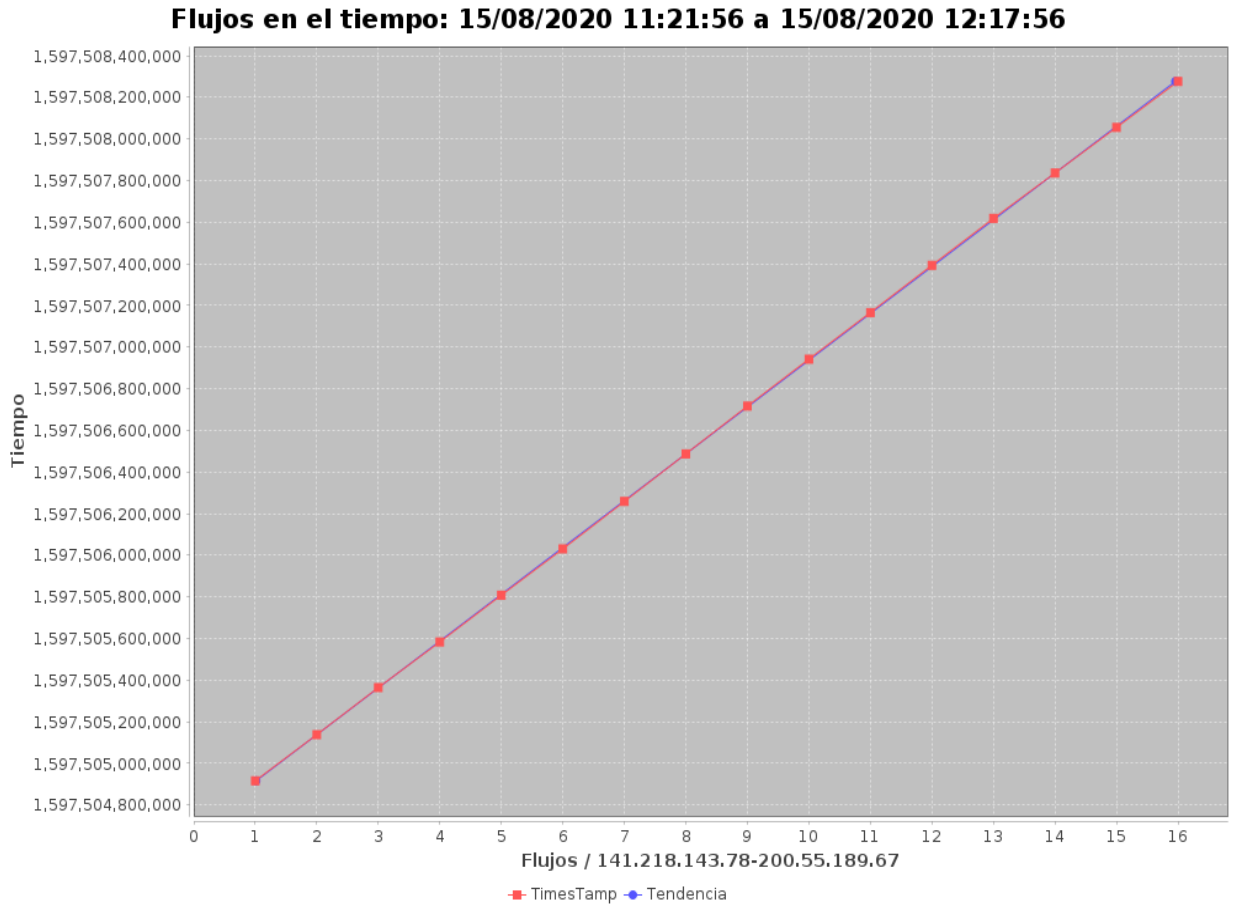

Figura 2: Conexiones IP 141.218.143.78.

Caso de muestra: IP 35.186.241.51

Dirección registrada a un centro de datos para hospedaje a nombre de Google LLC, ha sido reportada en AbuseIPDB en seis ocasiones (figura 3).

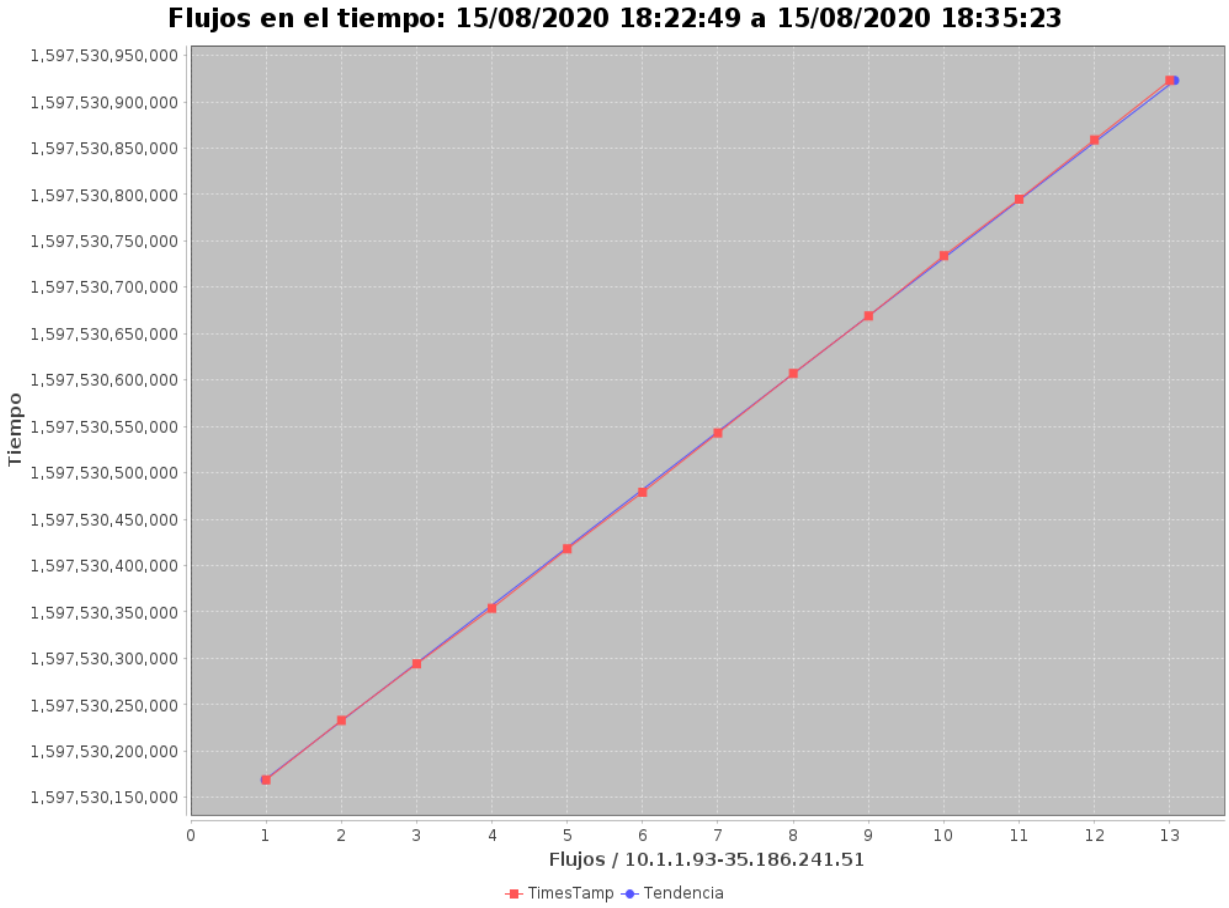

Figura 3: Conexiones IP 35.186.241.51.

Caso de muestra: IP 4.4.4.4

Dirección registrada en el dominio level3.com, perteneciente a *Level 3 Communications Inc*. Registrada en cuatro ocasiones en AbuseIPDB, pero su comportamiento no es periódico, por lo que se considera un falso positivo (Figura 4). Aquellas direcciones donde el número de conexiones es alto y frecuente, tiene tiempos entre arribo pequeños, por lo que el método la detectará al ser la desviación estándar baja, debe ser descartado al tratarse de un falso positivo.

TELEMÁTICA
REVISTA DIGITAL de las Tecnologías de la Información y las Telecomunicaciones
Revista Telemática. Vol.20 No.1, Enero- Marzo, 2021, p.27-35 ISSN 1729-3804

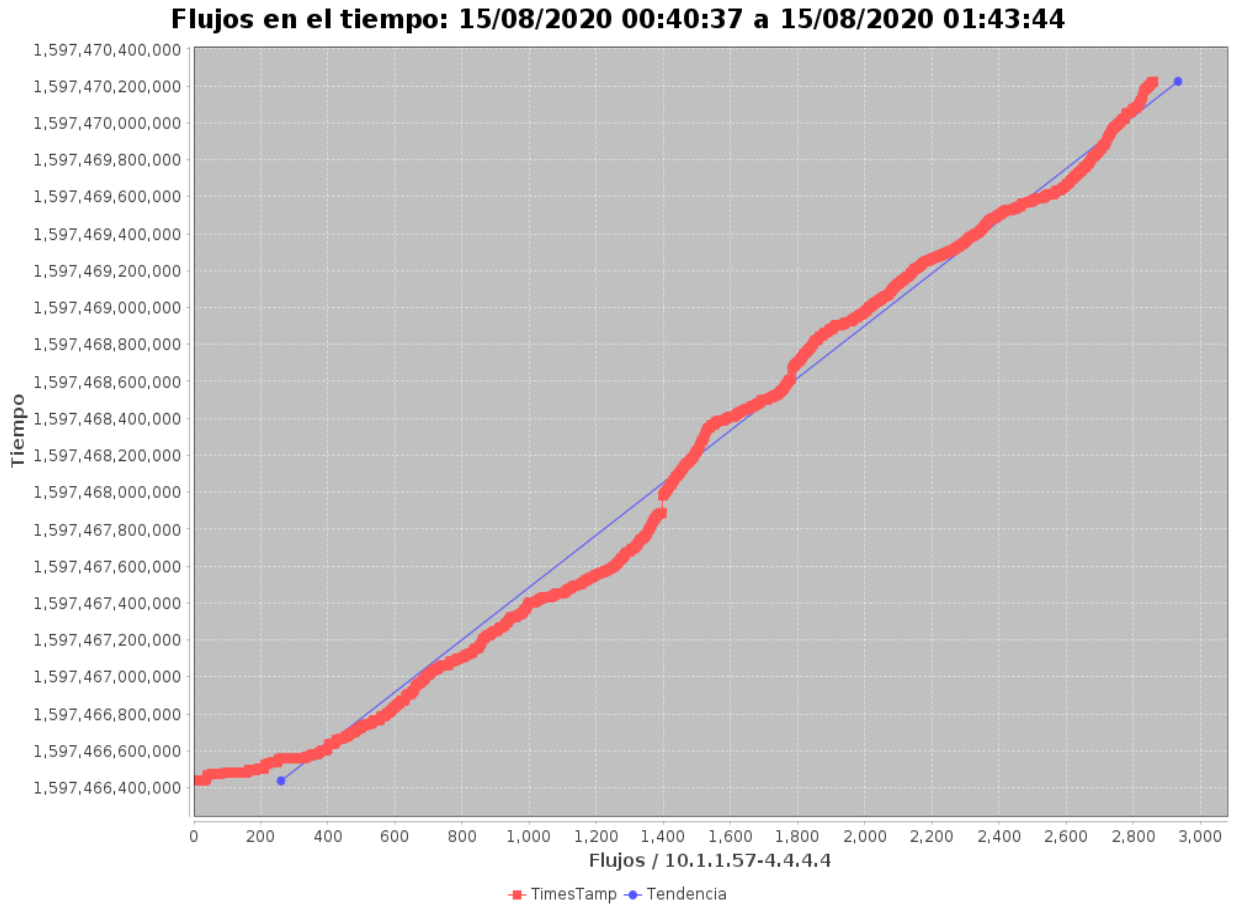

Figura 4: Conexiones IP 4.4.4.4.

Caso de muestra: IP 38.113.165.110

Dirección registrada a nombre de ksn-url.geoksn.kaspersky.com, correspondiente al servicio de Kaspersky Security Network, diseñada para recibir y procesar eventos de seguridad de los productos de Kaspersky Labs. La red analizada tiene como política de seguridad no permitir los reportes de funcionamiento de las aplicaciones. Al analizar un servidor de Kaspersky Antivirus, se comprueba que se encontraba activada la opción de enviar información a la red KSN, lo cual fue desactivado (Figura 5).

Este gráfico (Figura 5) fue generado con una de las primeras versiones de la herramienta, con una tecnología diferente, desafortunadamente, las trazas originales no se preservaron debido a problemas de espacio de almacenamiento y política de rotación de trazas. Se considera importante publicar debido a que es la principal evidencia disponible para validar el método.

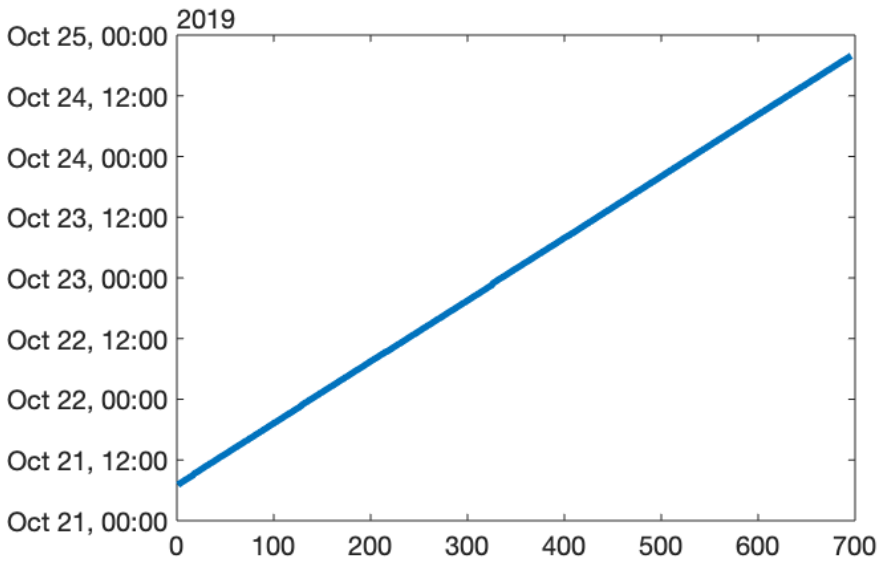

Figura 5: Conexiones IP 38.113.165.110.

Como resultado de la aplicación del método propuesto, de las cinco muestras analizadas, se detectan dos que son reportadas por AbuseIPDB, lo que demuestra su efectividad y obliga, a los responsables de seguridad informática, a realizar una investigación más profunda al respecto. Por otra parte, en la quinta muestra, que es el caso de Kaspersky , se identifica una vulnerabilidad en la red bajo prueba, por lo que se puede pasar a su corrección inmediata. En la primera, asociada al centro de hospedaje de servicios en Francia, no reportada en AbuseIPDB, el resultado puede tomarse como una alerta que merece un análisis a posteriori. En la cuarta, por su parte, no se detecta periodicidad, arrojando un falso positivo, dado que no se ajusta a las condiciones impuesta por el método.

Obsérvese que, aunque el experimento se realizó a partir de un número de muestras bajas, es posible obtener una información de especial utilidad. No obstante, aunque fue demostrada su efectividad, posee limitaciones para detectar conexiones con una periodicidad intermitente (ej.: conexiones que se interrumpen el fin de semana) o cuando la periodicidad se establece entre varios intervalos regulares. En este sentido es necesario implementar algoritmos capaces de detectar casos más complejos.

4. CONCLUSIONES

En la investigación se ha implementado un método para la detección de posibles fugas de información de una red corporativa a partir de las trazas de flujos de red obtenidas en el perímetro. Fue capaz de reconocer conexiones provenientes de un servicio mal configurado, detectándose también un caso de fuga de información. El método propuesto, aunque relativamente efectivo, es básico, presentando limitaciones, por lo que es necesario profundizar en la selección de los parámetros y la implementación de nuevos algoritmos para la detección de casos más complejos.

RECONOCIMIENTOS

El autor desea agradecer a la Fiscalía General de la República y al Departamento de Telemática de la Facultad de Telecomunicaciones de la Universidad Tecnológica de La Habana por sus aportes a la consecución de este trabajo.

REFERENCIAS

[1] V. Diaz, “THREAT PREDICTIONS FOR 2019,” 2019. [Online]. Available: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/11/27082929/KSB_Predictions-2019_General-APT.pdf.

[2] “Global surveillance - Universitetsbiblioteket,” 2016. https://www.ub.uio.no/fag/naturvitenskap-teknologi/informatikk/faglig/bibliografier/no21984.html (accessed Mar. 17, 2020).

Revista Telemática. Vol.20 No.1, Enero- Marzo, 2021, p.27-35 ISSN 1729-3804

[3] M. Marchetti, F. Pierazzi, M. Colajanni, and A. Guido, "Analysis of high volumes of network traffic for Advanced Persistent Threat detection," *Comput. Networks*, vol. 109, pp. 127–141, Nov. 2016, doi: 10.1016/j.comnet.2016.05.018.

[4] N. A. Huynh, W. K. Ng, and H. G. Do, "On periodic behavior of malware: Experiments, opportunities and challenges," in *2016 11th International Conference on Malicious and Unwanted Software, MALWARE 2016*, Mar. 2017, pp. 85–92, doi: 10.1109/MALWARE.2016.7888733.

[5] B. AsSadhan and J. M. F. Moura, "An efficient method to detect periodic behavior in botnet traffic by analyzing control plane traffic," *J. Adv. Res.*, 2014, doi: 10.1016/j.jare.2013.11.005.

[6] J. Ahmed, H. H. Gharakheili, C. Russell, and V. Sivaraman, "Real-time detection of DNS exfiltration and tunneling from enterprise networks," *Proc. IFIP/IEEE IM, Washingt. DC, USA*, 2019.

[7] J. Van Splunder, "Periodicity detection in network traffic," *Tech. Report, Math. Inst. Univ. Leiden*, 2015.

[8] "Math – Commons Math: The Apache Commons Mathematics Library." https://commons.apache.org/proper/commons-math/ (accessed Sep. 04, 2020).

[9] "AbuseIPDB making the internet safer, one IP at a time." https://www.abuseipdb.com/ (accessed Sep. 04, 2020).

SOBRE LOS AUTORES

Javier Alfonso Valdés: Segundo Jefe de la Dirección de Informática y Comunicaciones de la Fiscalía General de la República de Cuba. Profesor de programación a tiempo parcial en la Facultad de Telecomunicaciones y Electrónica de la Universidad Tecnológica de La Habana. Identificador ORCID: 0000-0001-7354-2861. Categoría docente: Instructor.

CONFLICTO DE INTERESES

Declaro que no existe conflicto de intereses de los autores o instituciones con relación al contenido publicado.