https://doi.org/10.22201/dgtic.ctud.2024.2.3.67

Vol. 2, Núm. 3. julio-septiembre 2024, págs. 32 - 39

Detección de malware utilizando un analizador de tráfico de red

Información del reporte:

Para citar este reporte técnico:

Pérez Santillán, P.T. (2024). Detección de malware utilizando un analizador de tráfico de red. Cuadernos Técnicos Universitarios de la DGTIC, *2* (3) páginas (x-y).

https://doi.org/10.22201/dgtic.ctud.2024.2.3.67

Pedro Temachti Pérez Santillán

Dirección General de Cómputo y de Tecnologías de Información y Comunicación

Universidad Nacional Autónoma de México

ptsantillan@gmail.com

ORCID: 0009-0000-2626-9073

Resumen

Cada método de detección y protección de malware tiene sus limitaciones, por lo que el uso de herramientas complementarias entre sí es fundamental para establecer una estrategia de defensa robusta y completa. Se utilizó un analizador de tráfico de red para buscar Indicadores de Compromiso (IoC) que permitieran identificar si un archivo analizado contenía código malicioso y posteriormente brindará información relevante del ataque. Durante este proceso se utilizó el software de distribución libre y multiplataforma Wireshark con los filtros DNS, HTTP y TCP que permitió encontrar patrones de comunicación inusuales e intentos de acceso a recursos no autorizados. Se demostró que esta aproximación es eficiente y puede traer beneficios a una estrategia integral de seguridad que pudiera ser utilizada en un futuro por el Centro de Datos.

Palabras clave:

Wireshark, malware, indicadores de compromiso, IoC, ciberseguridad, tráfico de red, análisis del protocolo DNS, análisis del protocolo HTTP, análisis del protocolo TCP, análisis de los objetos transmitidos.

https://doi.org/10.22201/dgtic.ctud.2024.2.3.67 Vol. 2, Núm. 3. julio-septiembre 2024, págs. 33 - 39

1. INTRODUCCIÓN

Las amenazas de malware están en constante evolución. La detección temprana y eficiente de un ataque es crucial para proteger datos y sistemas. Los métodos tradicionales de detección están basados comúnmente en firmas y filtros. Esto presenta limitaciones ante ataques sofisticados y ataques de día cero que no han sido agregados a las bases de firmas.

El concepto de utilizar analizadores de tráfico de red en ciberseguridad ya se ha utilizado anteriormente para la detección de intrusos (Banerjee et al., 2018). Si bien ese experimento se enfocó en el filtrado del ACL (*Access Control List*) efectuando una labor similar a la de un firewall, se encontró que este tipo de análisis tiene aplicaciones interesantes en materia de ciberseguridad.

Para probar la eficiencia de este enfoque se ejecutó un archivo infectado en una máquina virtual para posteriormente analizar el comportamiento de red del dispositivo.

El objetivo del proyecto fue utilizar Wireshark como una alternativa para buscar Indicadores de Compromiso (IoC) en un equipo infectado por un archivo malicioso y demostrar que el análisis de tráfico de red puede ser una herramienta útil en un esquema integral de ciberseguridad.

Wireshark es una herramienta de análisis de tráfico de red, por medio de su utilización es posible tener una perspectiva diferente para la detección de malware en el sistema al identificar patrones de comportamiento extraños. Si bien este método también tiene sus limitaciones, es una alternativa complementaria para poder detectar actividad sospechosa y tener una pronta reacción que permita reducir el impacto del ataque.

2. DESARROLLO TÉCNICO

Cada malware tiene un método de ataque diferente, dependiendo de las vulnerabilidades que busque explotar y la intención del ataque, será el comportamiento que presente el dispositivo infectado. Un dispositivo infectado podría permanecer sin ningún tipo de comportamiento extraño por meses, pero comúnmente tratará de avisar al atacante que ha sido exitoso y mandar información del sistema. Algunos tipos de malware solamente abren un canal de entrada al dispositivo infectado para posteriores ataques y reportan su dirección. El tipo de información es lo que se buscó en el análisis.

El flujo de información capturado por Wireshark puede llegar a ser muy extenso para analizarlo de manera detallada. Fue importante definir primero una metodología que permitiera revisar de manera sistemática los protocolos más importantes en busca de Indicadores de Compromiso (IoC). En este proceso, partiendo de dichos indicadores, se pueden tomar diversos caminos para seguir el rastro de alguna actividad sospechosa.

Un estudio reciente (Singh y Singh, 2021) plantea dos aproximaciones para el análisis del tráfico de la red en busca de señales de un ataque: enfocado al flujo de red y/o a los paquetes. De manera que se hizo una revisión de los protocolos comúnmente utilizados en ataques en los que Wireshark ha mostrado ofrecer un análisis completo y detallado (Saxena y Sharma, 2017) y posteriormente una revisión del contenido de paquetes sospechosos y objetos transmitidos.

https://doi.org/10.22201/dgtic.ctud.2024.2.3.67 Vol. 2, Núm. 3. julio-septiembre 2024, págs. 34 - 39

Los pasos que siguió la metodología para la identificación del malware fueron:

- Análisis del protocolo DNS
- Análisis del protocolo HTTP
- Análisis del protocolo TCP
- Análisis de los objetos transmitidos

2.1 METODOLOGÍA

2.1.1 PREPARACIÓN DEL ENTORNO DE TRABAJO

Es importante contar con un ambiente de trabajo seguro y aislado del resto del sistema cuando se trabaja con un archivo que podría contener malware. Se utilizó VirtualBox corriendo Windows 10 para generar un entorno virtual seguro.

La configuración de red que se utilizó para la conexión de la máquina virtual fue *Bridged Adapter*, que conectará a la máquina virtual como un elemento más de la red, de manera que tenga una dirección IP propia y no genere confusión con el tráfico generado por la computadora anfitriona.

Para realizar las pruebas se utilizó un archivo infectado con el malware *Trickbot*. La Agencia de Ciberdefensa de América ofrece información adicional de este malware (Cybersecurity Advisory, 2021). Para replicar este tipo de experimentos, en los repositorios de Github o bases de datos de amenazas de ciberseguridad es posible encontrar archivos infectados que se utilizan para fines académicos.

Se utilizó Wireshark version 4.2.5, y la captura del tráfico de red se comenzó un par de minutos antes de infectar la máquina virtual. Se limitó en la medida de lo posible toda actividad innecesaria tanto en la máquina virtual como en la máquina anfitriona, con la finalidad de reducir el tráfico a analizar.

2.1.2 ANÁLISIS DEL PROTOCOLO DNS

El protocolo DNS (Sistema de Nombres de Dominio) permitió obtener la dirección IP de una página o sitio web al cual queremos acceder: es el primer lugar donde podremos encontrar actividad de parte del malware. A menudo en este tipo de ataques, nuestro equipo se comunica con servidores de Comando y Control (C&C o C2) para recibir instrucciones o enviar datos robados. Estos C&C pueden alojarse en servicios de *hosting* anónimos al cual el atacante tendrá acceso y nuestro dispositivo realizará una consulta de DNS para acceder a ellos. Identificar este tipo de comunicación puede ser un indicio de la presencia de malware.

De igual forma, se buscan patrones de tráfico sospechoso, por ejemplo, si se realiza un gran número de solicitudes DNS de dominios desconocidos o páginas web a las que no hayamos accedido.

2.1.3 ANÁLISIS DEL PROTOCOLO HTTP

El siguiente paso fue revisar el protocolo HTTP (Protocolo de Transferencia de Hipertexto). Las conexiones a servidores remotos comúnmente utilizarán este protocolo. Cuando un paquete resulta sospechoso,

https://doi.org/10.22201/dgtic.ctud.2024.2.3.67 Vol. 2, Núm. 3. julio-septiembre 2024, págs. 35 - 39

Wireshark nos permite hacer un seguimiento detallado del flujo TCP de la comunicación (TCP stream). Un dispositivo infectado comúnmente tratará de enviar nuestras credenciales, llaves y contraseñas al atacante. No se debe confundir cuando vemos que las credenciales de acceso y autenticación son utilizadas para realizar una conexión legítima a algún servicio.

La opción de Geolocalización es un complemento que se puede instalar en Wireshark para darnos información adicional respecto a la ubicación de las direcciones IP a las que los dispositivos tratan de conectarse (Chappell, 2019). Esta información no es contundente, pero ayuda a definir el panorama.

Al navegar en diferentes sitios utilizando HTTP, comúnmente utilizarán el puerto 443 en lugar del puerto 80. Algunas aplicaciones aún trabajan el puerto 80, pero cuando se ven muchos paquetes a través de este puerto, es necesario hacer una revisión más profunda.

2.1.4 ANÁLISIS DEL PROTOCOLO TCP

Posteriormente se revisaron las peticiones *Hello*, que es el primer paso cuando se realiza una solicitud de conexión TLS (Seguridad de la Capa de Transporte). Una versión obsoleta de la conexión podría ser un indicio de actividad maliciosa. La solicitud de conexión TLS generará un código JA3. Esta firma de conexión puede ser comparada en bases de datos en búsqueda de indicios de conexiones maliciosas. Si bien no es un método infalible, se ha encontrado que esta información puede ser de utilidad para detectar el tipo de conexión que se establece (Roques et al., 2019).

Un aumento repentino en el volumen de tráfico TCP, especialmente hacia servidores externos, podría ser indicativo de actividad maliciosa, como la transmisión de información robada de nuestro dispositivo. Cuando se presentan anomalías en los tiempos de respuesta como que éstos sean inusualmente largos podrían indicar la presencia de un intermediario en la comunicación ejecutando un ataque *man-in-the-middle*.

2.1.5 ANÁLISIS DE LOS OBJETOS TRANSMITIDOS Y EL CONTENIDO DE LOS PAQUETES

Por medio de la opción de exportación de objetos HTTP, será posible ver todos los elementos que fueron enviados a través de este protocolo, lo que permitirá inspeccionar el flujo de los paquetes que contenga un archivo que llame nuestra atención y analizarlo en búsqueda de código malicioso, scripts o datos sospechosos.

Algunos tipos de malware tratarán de propagarse, enviando el código malicioso a otros dispositivos. Se recomienda ser muy cuidadosos con los archivos encontrados. Cuando algún archivo llame nuestra atención, se debe enviar a alguna base de datos como VirusTotal para verificar si está infectado.

2.2 RESULTADOS

Del análisis del protocolo DNS:

Se inició aplicando el filtro *DNS*. Se realizó una inspección en todas las peticiones que el equipo está realizando.

https://doi.org/10.22201/dgtic.ctud.2024.2.3.67 Vol. 2, Núm. 3. julio-septiembre 2024, págs. 36 - 39

El dispositivo infectado realizó una solicitud DNS al sitio *wtfismyip.com*, un sitio que proporciona la dirección IP del equipo y suele estar asociado con actividad maliciosa (Any Run, 2021).

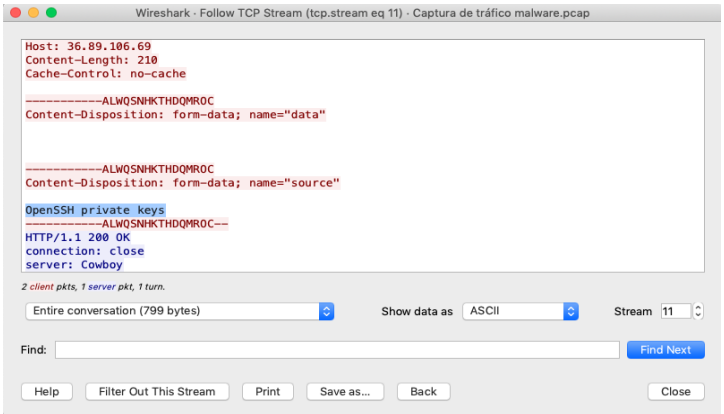
Del análisis del protocolo HTTP:

Se encontró que nuestro dispositivo buscaba conectarse a un servidor llamado Cowboy. El nombre de este servidor ha estado asociado a ataques de malware (Cybersecurity Advisory, 2021). Con el filtro *ip.addr* se encontró que dicho servidor estaba asociado a la dirección IP 173.166.146.112.

A este servidor se le enviaba información del sistema operativo de nuestro dispositivo y encabezados que indican que el ataque apuntaba a nuestras contraseñas de Outlook, credenciales de OpenSSH (Figura 1) y OpenVPN, así como información bancaria.

Figura 1

El encabezado muestra que el atacante está apuntando a obtener nuestras llaves OpenSSH

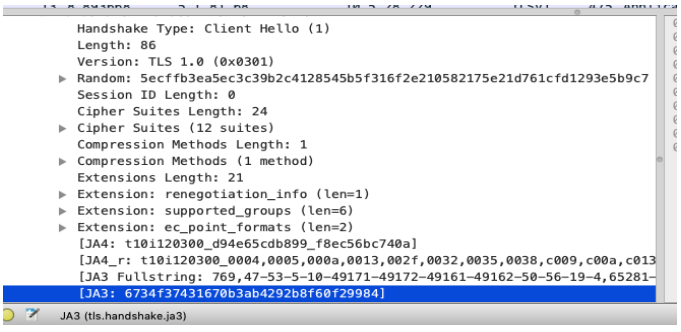


Del análisis del protocolo TCP:

Se encontró una conexión TLS que llamaba la atención por utilizar una versión muy antigua; la firma *JA3* (Figura 2) de esta conexión había sido reportada como sospechosa de malware en una base de datos de IoC (Althouse, 2019).

Figura 2

Firma JA3 de la conexión TLS que se revisó



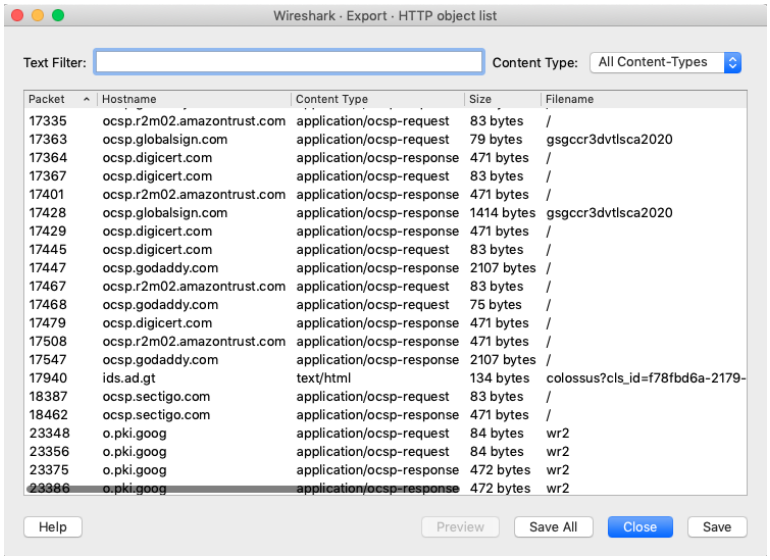
https://doi.org/10.22201/dgtic.ctud.2024.2.3.67 Vol. 2, Núm. 3. julio-septiembre 2024, págs. 37 - 39

Del análisis de los objetos transmitidos y el contenido de los paquetes se encontró lo siguiente:

La lista de objetos transmitidos durante el análisis arrojó que la mayoría fueron respuestas de aplicaciones (Figura 3).

Figura 3

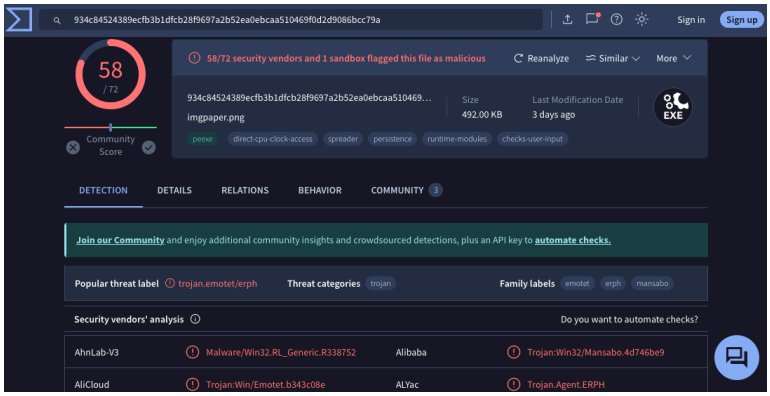
Inspección de los objetos HTTP encontrados en la captura de tráfico de red



Sin embargo se encontraron dos archivos con extensión PNG. A pesar de que las páginas web presentan todo tipo de imágenes, éstas normalmente no aparecen como objetos en el flujo de datos. Se descargó y se analizó en VirusTotal (VirusTotal, 2024), encontrando que el archivo contenía código malicioso (Figura 4).

Figura 4

Resultados del análisis del archivo extraído



https://doi.org/10.22201/dgtic.ctud.2024.2.3.67 Vol. 2, Núm. 3. julio-septiembre 2024, págs. 38 - 39

Utilizando el filtro *frame contains ".exe"* se revisó si algún paquete transmitía información de procesos del sistema. Se encontró que uno de los paquetes efectivamente contenía esta información. El atacante intentaba obtener información de procesos corriendo en nuestro sistema (Figura 5).

Figura 5

Procesos de nuestro sistema de los que se le está informando al atacante

Se encontraron varios Indicadores de Compromiso (IoC) con los que se pudo concluir que efectivamente la máquina había sido infectada. Dentro del análisis se encontraron indicios de lo que el atacante pretendía hacer en el equipo, incluyendo una dirección IP a la que nuestro dispositivo buscaba conectarse y un objeto infectado con el que el malware podría haberse replicado.

La metodología utilizada es una manera eficiente de buscar IoC en el tráfico de la red y pudiera funcionar como referencia para continuar desarrollando diversos métodos. El análisis de tráfico de red demostró ser una herramienta útil para las medidas de seguridad de un equipo de cómputo, que puede complementar y aportar valor en la identificación de malware y detección de dispositivos infectados a métodos tradicionales.

3. CONCLUSIONES

Los analizadores de tráfico de red son una excelente herramienta para el análisis de malware y para diagnosticar cuando un equipo ha sido infectado. Si el ataque ha podido evitar nuestras defensas, el comportamiento del equipo ofrecerá información valiosa para su detección. Este proceso puede llevarse a cabo de manera posterior como una especie de análisis forense o método de detección de malware, así como en tiempo real.

El punto más vulnerable de un sistema informático sigue siendo sus usuarios. Aunque nuestra red cuente con protocolos robustos, a través de un correo o un archivo externo estos pueden abrir una brecha de seguridad. La detección de un ataque por medio del tráfico de red, brinda la posibilidad al administrador de detectarla de manera remota, sin necesidad de acceder al dispositivo del usuario.

https://doi.org/10.22201/dgtic.ctud.2024.2.3.67 Vol. 2, Núm. 3. julio-septiembre 2024, págs. 39 - 39

AGRADECIMIENTOS

A Patricia Santillán, por todo su apoyo en los proyectos que me trajeron a este punto.

REFERENCIAS

Althouse, J. (2019). TLS Fingerprinting with JA3 and JA3S. https://engineering.salesforce.com/tls-fingerprinting-with-ja3-and-ja3s-247362855967/

Any Run. (2021). *Wtfismyip General Info*. https://any.run/report/e3d78e7428ee28a4276fbb76dee1af0d361aa7608add631e48d1066f6acb91b2/a68cc05c-55b9-4a7a-9566-9df232134fcb

Banerjee, U., Vashishtha, A., & Saxena, M. (2010). Evaluation of the Capabilities of WireShark as a tool for Intrusion Detection. *International Journal of computer applications*, *6*(7), 1-5.

Chappell, L. (2019). *GeoIP Mapping in Wireshark*. https://www.chappell-university.com/post/geoip-mapping-in-wireshark

Cybersecurity Advisory. (2021). *TrickBot Malware*. Cybersecurity and Infrastructure Security Agency https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-076a

Roques, O., Maffeis, S., & Cova, M. (2019, September). Detecting malware in TLS traffic. In *The IEEE Conference on Local Computer Networks 30th Anniversary (LCN'05,* pp.*12-13)*.

Saxena, P., & Sharma, S. K. (2017). Analysis of network traffic by using packet sniffing tool: Wireshark. *International Journal of Advance Research, Ideas and Innovations in Technology*, *3*(6), 804-808.

Singh, A. P., & Singh, M. (2021). A comparative review of malware analysis and detection in HTTPs traffic. *International Journal of Computing and Digital Systems*, *10*(1), 111-123.

VirusTotal. (s.f.). *Upload*. https://www.virustotal.com/gui/home/upload