TELEMÁTICA
REVISTA DIGITAL de las Tecnologías de la Información y las Telecomunicaciones
Revista Telemática. Vol. 17. No. 2, mayo-agosto, 2018, p.1- 12 ISSN 1729-3804

SOLUCIÓN DE CIBER-SEGURIDAD PERIMETRAL PARA REDES DE DATOS EMPRESARIALES

Ing. Asiel E. Hernández Cervantes [1], Ing. José L. Chamizo Hechavarría [2]

[1] XETID (Empresa de Tecnologías de la Información para la Defensa). División de Ciber-Seguridad y Tecnologías Bancarias. Calle 296 entre Ave. 207 y 203. Boyeros, La Habana,
[2] XETID (Empresa de Tecnologías de la Información para la Defensa). División de Ciber-Seguridad y Tecnologías Bancarias. Calle 296 entre Ave. 207 y 203. Boyeros, La Habana, Cuba.
[1] asielenrique@xetid.cu:

RESUMEN

Durante los últimos años se ha producido un crecimiento notable en los riesgos, vulnerabilidades y amenazas en la red. Esto acompañado a la diversidad de dispositivos que hoy día se conectan en los ambientes empresariales y a la escasez de personal especializado en seguridad informática, dificulta grandemente la protección y seguridad de las entidades. El desarrollo e implementación de una solución de software y hardware para seguridad perimetral, que sea capaz de proteger todo el tráfico de entrada y salida de las redes informáticas empresariales, así como, intercambiar de forma distribuida la información de seguridad con otras entidades nacionales, asegura sustancialmente el nivel de protección de los datos y activos en la red. En adición permite contrarrestar con mayor rapidez y efectividad las amenazas que afectan al país. Esta solución integra elementos de enrutamiento y filtrado de paquetes, descubrimiento y prevención contra intrusos en tiempo real, análisis y filtrado de contenidos, detección y análisis automatizado de malware y virus en la red, así como otras herramientas para la configuración y la gestión de la seguridad informática. Además, se encarga de brindar la información sobre los atacantes y tipos de ataques detectados al resto de las soluciones desplegadas. De esta forma se logra proteger contra atacantes más rápidamente, logrando así el incremento de la ciber-seguridad de las infraestructuras tecnológicas del país.

PALABRAS CLAVE: Aplicaciones, Hardware, Perimetral, Proteger, Ciber-seguridad.

CIBER-SECURITY PERIMETRAL APPLIANCE FOR EMPRESARIAL NETWORKS

ABSTRACT

Nowadays, the increase on risks, vulnerabilities and threats on computer network results of major importance to properly preserve performance and security. Besides, considering the variety of devices currently connected on corporative environments and the shortage of technical workers on computer security, hampers greatly the protection and security tasks in case of entities dealing with ICT

technologies. The development and implementation of software for perimeter security, capable of protecting all incoming and outgoing traffic from corporate computer networks, as well as, interchanging distributed security information with other national entities, substantially ensure levels of protection of data and assets on the network. In addition, it makes possible to counteract threats that affect the country more quickly and effectively. This solution integrates routing and packet filtering elements, realtime intrusion detection and prevention, content analysis and filtering, automated detection and analysis of malware and viruses on the network, and other tools for configuration and management of computer security. In addition, it is responsible to provide information concerning attackers and types of attacks detected to the rest of the deployed solutions. Thus, this solution may protect more quickly, which in turn increases cyber-security regarding technological infrastructure of the country.

KEYWORDS: Software, Hardware, Perimeter, Protection, Ciber-security.

INTRODUCCIÓN

La informática y las telecomunicaciones se encuentran entre los sectores que han experimentado los cambios más significativos en los últimos 50 años, provocando a su vez, el desarrollo de las tecnologías, los métodos y los recursos humanos que interactúan con ellas. Cada vez son mayores las industrias, empresas y entidades que tienen presencia y/o interacción en Internet, y en ocasiones, algunas que solo existen en torno a esta. Ello ha generado la necesidad de tener en línea todo tipo de información, desde los archivos multimedia personales, hasta las líneas y proyectos de negocios de grandes empresas.

La protección de toda información relativa a la operación de la empresa ha pasado a ocupar un lugar primordial en los intereses y presupuestos de las entidades. Sin embargo, contar con los especialistas preparados para hacer frente a la creciente expansión de las amenazas en la red, puede ser en algunos casos, extremadamente costoso, y en otros, muy difíciles de encontrar. No obstante, existen muchos proyectos en desarrollo y explotación, que pueden minimizar los tiempos de detección y reacción ante incidentes informáticos dentro de las infraestructuras, facilitando además las labores de gestión de los administradores de sistemas, aunque la puesta a punto y explotación suele ser bastante complicada.

Debido a esos factores, se decidió implementar una solución integral (denominada “appliance”) que combine hardware de servicio profesional y herramientas de seguridad de software libre, con el objetivo de proteger el perímetro de las infraestructuras de redes de comunicaciones locales. Dicha solución debe ser capaz de incorporarse de manera transparente y/o sustituir en las redes que los requieran, las funciones de los dispositivos de entrada y salida presentes en la red a asegurar. Además, este appliance, se integrará a través de un Centro de Comando y Control de Seguridad (C&C), con el resto de los dispositivos desplegados, y tributará/recibirá la información necesaria para garantizar la respuesta oportuna ante las nuevas amenazas.

DESCRIPCIÓN DE LA PROPUESTA DE APPLIANCE

El objetivo de la investigación es implementar una solución de seguridad perimetral por hardware "appliance" capaz de asegurar el tráfico de entrada y salida de las redes internas de las entidades. Por tanto, inicialmente es necesario definir el tipo de dispositivo de hardware a emplear. Se debe elegir un dispositivo que sea capaz de hospedar las diferentes aplicaciones que garantizarán los elementos de

seguridad que posteriormente serán incorporados, lo que deriva la necesidad que el equipo posea buenas características de rendimiento, dimensionadas, por los flujos de tráfico (definidas por el ancho de banda de las entidades, así como los servicios brindados y/o consumidos desde internet) que serán protegidos, así como el consumo de recursos de sus aplicativos internos. Como parte de la solución estarán incorporados dentro del appliance los servidores de:

- Pfsense [1]. La documentación oficial de los desarrolladores del software define el consumo de recursos de este aplicativo, según el tráfico de red y los servicios internos que brinde, varía entre 512 MB - 2 GB de memoria RAM aproximadamente, así como, de 1 - 8 GHz de CPU. El tamaño en disco se corresponde con la rotación interna de los logs autogenerados, así como de algunas funcionalidades de salva de tráfico.
- Suricata IDS/IPS [2]. El consumo de recursos de este software es menos preciso, puesto que puede variar por la cantidad de tráfico de red que monitoriza, el tipo de dicho tráfico, así como por el modo de funcionamiento que emplea (IDS o IPS). Se recomienda emplear siempre un mínimo de 4 GB de memoria RAM y 8 GHz de CPU, para correr este aplicativo, así como realizar un análisis en el tiempo del comportamiento del software y ajustar los recursos asignados en función de su rendimiento y de la escalabilidad de la infraestructura de red que monitoriza. El tamaño en disco se corresponde con la rotación interna de los logs autogenerados, así como de algunas funcionalidades de salva de tráfico.
- Moloch [3]. Los desarrolladores recomiendan en su sitio oficial, asignarle no menos de 8 GB de memoria RAM y 8 GHz de CPU para su correcto funcionamiento, aunque puede variar en correspondencia con el flujo de tráfico que monitorice. En el caso de este software el tamaño en disco es prácticamente despreciable puesto que su información se almacena en una base de datos externa con el objetivo de realizar otros análisis.
- Cuckoo Sandbox [4]. El consumo de este aplicativo está definido fundamentalmente por la cantidad de instancias de análisis y simulación que corran dentro del mismo. Se debe establecer una relación de compromiso entre las instancias que se desean correr simultáneamente y los recursos asignados al aplicativo. Se recomienda emplear un mínimo de 4 GB de memoria RAM y 4 GHZ de CPU para el funcionamiento de 4 instancias de análisis simultáneamente. El tamaño en disco de este software varía según el tipo y la permanencia en el tiempo, de los informes de resultados de los análisis que realice.
- Xplico [5]. Los recursos asignados a este aplicativo se corresponderán con los flujos de tráfico que analizará, sin embargo, se le deben asignar no menos de 2 GB de memoria RAM y 2 GHZ de CPU para su funcionamiento. El tamaño en disco de esta solución está en correspondencia con la perdurabilidad de los ficheros que el mismo reconstruya.

Otro aspecto fundamental, es la cantidad y el tipo de las interfaces de red que poseerá el appliance, con el objetivo de mantener los estándares de calidad de servicio, y asegurar la capacidad de serviciar varias subredes locales internas. Producto de los análisis preliminares realizados se determinó que era necesario contar con un dispositivo físico capaz de brindar un mínimo de 20 GB de memoria RAM y 30 GHZ de CPU para sus aplicativos internos y que contara además con la habilidad de incorporar interfaces de red profesionales.

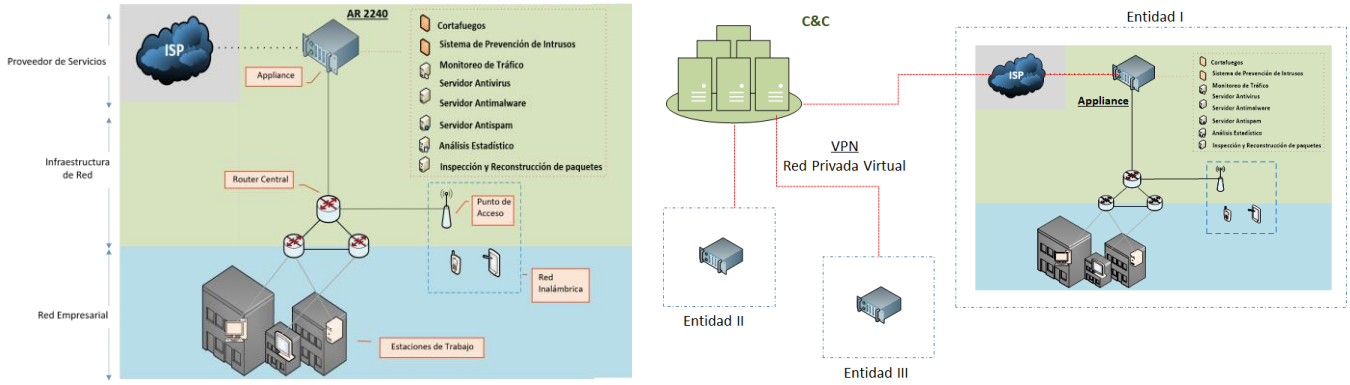
Luego de un análisis del equipamiento presente en las instituciones nacionales, así como, las facilidades de adquisición del equipamiento de proveedores extranjeros, se decidió implementar la solución empleando tecnología de la empresa china “Huawei”. Dentro de la diversidad de tecnologías brindadas por el fabricante Huawei, se eligió el dispositivo AR2240. Este equipo tiene una arquitectura modular, lo cual permite incorporarle bajo demanda, los elementos necesarios para garantizar las necesidades de

recursos de sus aplicativos internos, así como, las interfaces de red necesarias. Además, este dispositivo trae incluido como módulo de salida un router profesional, con interfaces de red en modo combo (que soportan interfaces de cobre e interfaces de fibra óptica), capaces de brindar altos parámetros de calidad de servicio durante el manejo de los flujos de tráfico [6].

Para brindar los servicios de seguridad perimetral el appliance tiene las características de:

a. Enrutador de tráfico de red.
b. Servidor Cortafuego.
c. Sistema de Detección y Prevención de Intrusiones.
d. Servidor Antivirus y Antimalware.
e. Servidor de Monitoreo de Tráfico.
f. Servidor Antispam.
g. Servidor de Inspección y Reconstrucción de paquetes.
h. Análisis estadístico.

El modo de funcionamiento de la solución es como se muestra en la siguiente Figura 1. A su vez el appliance debe ser capaz de reportar hacia un Centro de Comando y Control (C&C) de Seguridad los indicadores de compromiso (IoC) detectados en la infraestructura que monitoriza. El C&C se encargará además de realizar la actualización automática, al resto de los appliance desplegados, de los IoC que están afectando a las infraestructuras, con el objetivo de responder con mayor rapidez y oportunidad a los ataques y/o amenazas que afectan el entorno nacional.



a) b)

Figura 1. a) Modelo de funcionamiento de la Solución. b) Modelo de integración nacional.

Arquitectura de la Solución

El appliance se diseñó y configuró de forma tal, que cada una de las herramientas que integra, tenga acceso a la información que necesita para realizar sus labores de seguridad. Garantizando además que estas no influyan negativamente sobre los parámetros de QoS presentes en la red que vaya a proteger. Además, debe ser capaz de incorporarse de forma transparente en la infraestructura que monitorice, o en casos, en que se requiera, sustituir el dispositivo perimetral de la entidad. La arquitectura lógica de la solución es como se muestra en la Figura 2.

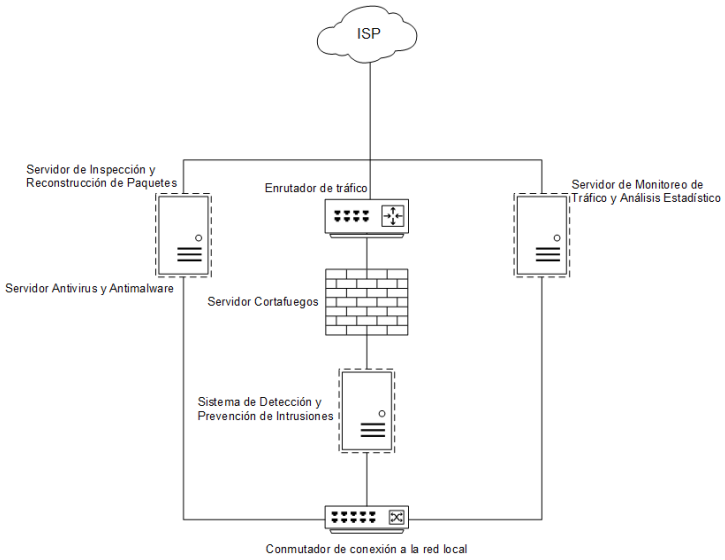


Figura 2. Arquitectura lógica del appliance.

Enrutador de tráfico

El servicio de enrutamiento de paquetes es imprescindible para la interconexión de infraestructuras de red. Los dispositivos capaces de realizarlo son aquellos que puedan trabajar en el denominado Nivel 3 del Modelo OSI, entre ellos encontramos: los enrutadores de paquetes (routers), los conmutadores de nivel 3 (L3 switchs) y los cortafuegos, estos últimos además de realizar el enrutamiento de los paquetes son capaces de bloquearlos y denegarlos según su contenido IP.

Esta solución emplea un enrutador del fabricante Huawei de la serie AR 2200, este equipo es capaz de realizar las labores de enrutamiento de tráfico, creación de ACLs, nating, balanceo de carga, tunelización VPN, limitación de anchos de banda, entre otros. Además, cuenta con soportes para incorporar tecnología GSM y 3G, Wifi, etc. Este dispositivo se encarga de realizar las labores de enrutamiento sin afectar la QoS de las redes serviciadas, puede realizarlo de forma transparente para la red de los clientes, e incorporar otras soluciones de red que se adapten a las nuevas tecnologías y faciliten la escalabilidad en el tiempo de la infraestructura que monitoriza.

Servidor Cortafuego

La solución cortafuegos implementada está basada en la solución de software libre pfSense, la cual se encarga de realizar las labores de filtrado y procesamiento de paquetes en las direcciones de entrada y salida de la infraestructura de red monitorizada. Los filtros implementados en el cortafuego se actualizan de forma automatizada sin interacción de los usuarios. Entre las funciones que realiza se encuentran:

- Filtrado de paquetes según las políticas de la entidad.
- Filtrado automatizado de paquetes según su Reputación IP.
- Filtrado de dominios.
- Filtrado de URLs.
- Bloqueo en tiempo real de los ficheros maliciosos detectados.

- Actualización automática de los filtros configurados.

Los metadatos empleados para realizar el filtrado del tráfico en el cortafuego son:

src_ip	src_port	protocol
dest_ip	dest_port	ip_reputation
url_domain		
url_address		
md5_file	url_filename	

Tabla 1. Metadatos de Filtrado en Cortafuego.

src_ip src_port protocol
dest_ip dest_port ip_reputation
url_domain
url_address
md5_file url_filename

Entre las herramientas instaladas y configuradas en el cortafuego se encuentran:

- Squid Proxy.
- SquidGuard.
- pfBlocker.
- Iperf.

Los principales sitios de reputación IP que emplea son:
- AlienVault [7].
- Emergingthreats [8].
- Blocklists [9].
- CIF [10].
- AlienVault OTX [11].
- Shallalist.

Sistema de Detección y Prevención de Intrusiones

La solución emplea como Sistema de Detección y Prevención de Intrusiones la herramienta de software libre Suricata, la cual, es un IDS de red, que se encarga de identificar firmas de amenazas conocidas, a partir del análisis de los datos que se intercambian en la red. Dicha herramienta contiene más de 65,000.00 reglas para detección de amenazas, incluyendo las libres, comunitarias y profesionales, e incorpora un gran número de disectores para la interpretación de la mayoría de los protocolos de red, entre ellos se destacan: http, smtp, ftp, telnet, dns, ntp, nfs, entre otros. Además, hace uso de las funciones multi-hilo de manera que solo con ejecutarse en una instancia realiza un balanceo de carga entre todos los procesadores disponibles.

Debido a estas funcionalidades, esta herramienta es capaz de procesar un ancho de banda de hasta 10 gigabits por segundo sin que ello repercuta sobre el rendimiento. Una de las principales fortalezas de este software es su capacidad de correr en modo IPS, lo cual le permite no solamente detectar las amenazas en la red, sino también, ser capaz de bloquearlas en tiempo real. Para ello, se configuró de forma tal que incorpora varios ficheros personalizados con las informaciones de reputación IP y los IoC detectados por el resto de las herramientas, así como, la información proveniente del resto de appliance desplegados en el país, a través de las actualizaciones del C&C. Estos ficheros se actualizan automáticamente, por lo que no requieren de la interacción de los administradores, y permiten que la solución sea capaz de responder con gran rapidez ante las amenazas emergentes en la infraestructura. Las reglas integradas en la herramienta permiten identificar fundamentalmente:

- Attack_response.
- Chat.
- Dns.
- Dos.
- Exploit.
- Ftp.
- Games.
- Imap.
- Inappropriate.
- Malware.
- Mobile_malware.
- Netbios.
- P2p.
- Policy.
- Pop3.
- Rpc.
- Scada.
- Scan.
- Shellcode.
- Smtp.
- Snmp.
- Sql.
- Telnet.
- Tftp.
- Trojan.
- User_agents.
- Voip.
- Web_client.
- Web_server.
- Web_specific_apps.
- Worm.
- Tor.

Esta herramienta genera además informes de seguridad con las principales amenazas que han afectado a la infraestructura. Los informes se envían, a través de un canal protegido, y anonimizando la

información de red interna, hacia el C&C, el cual la empleará para crear pulsos de IoC para el resto de appliance instalados, un ejemplo de esto se muestra en la Figura 4.

Figura. 3. Alerta de Suricata.

Servidor Antivirus y Antimalware

El appliance es capaz de determinar las firmas de virus e identificar indicadores de malware conocidos. Para realizar los análisis utiliza los paquetes reconstruidos desde el tráfico de red que es capturado por los otros componentes. El servicio de análisis está implementado de forma tal que se realiza de forma automatizada (de igual forma se puede ejecutar manualmente por los administradores), y emplea los motores antivirus de los desarrolladores:

- BitDefender
- Yara
- Virus Total
- Comodo
- Avast
- Kaspersky
- ClamAV

La solución implementa además un servicio de reconocimiento de amenazas, el cual está basado en el empleo de análisis automatizados, a partir de la simulación en entornos controlados de los ficheros a analizar. Para ello utiliza la herramienta de software libre “Cuckoo Sandbox”, la cual se encarga de realizar la simulación de la ejecución de los ficheros en instancias virtuales, con el objetivo de describir el comportamiento de los mismos, para identificar indicadores maliciosos, independiente de que no tenga firmas maliciosas asociadas.

Ambos procesos una vez reconocidas las firmas sospechosas, pueden generar un pulso con los IoC detectados. De esta forma las soluciones encargadas de la prevención de intrusiones puedan actualizar sus reglas para evitar la afectación de la amenaza detectada. Los IoC que pueden ser generados quedan ilustrados en la Tabla 2.

Tabla 2. Metadatos de Virus y Malware.

src_ip	src_port	protocol
dest_ip	dest_port	dns_servers
url_address		
know_sign[1]	filename	
reputation[2]	md5_file	
created_md5_files[3]	created_register_entries[4]	

Servidor Antispam

El servicio antispam se brinda a partir de las facilidades la identificación de las direcciones IP con reputación de envío de Spam, desde los sitios conocidos. Además identifica la información intercambiada a través de la inteligencia del resto de los appliance desplegados, combinado con la capacidad de bloqueo en tiempo real en el servidor cortafuego y en el sistema de prevención de intrusiones. La reputación de las direcciones IP asociadas con Spam, son actualizadas cada 15 minuntos en el servidor C&C nacional del appliance, y notificadas al mismo, cuando se identifica una dirección nueva. La reputación es revisada y limpiada (en caso de que proceda) de forma automatizada en el servidor de C&C nacional diariamente.

Servidor de Inspección y Reconstrucción de paquetes

Todos los análisis que se realizan de forma automatizada para identificar malware en los ficheros descargados/subidos en el tráfico de la entidad que atraviesan el appliance. Estos análisis se ejecutan a partir de la reconstrucción de los mismos desde las capturas de tráfico realizadas como se muestra en la Figura 4. Para ello se emplea la solución de software libre Xplico, la cual se encarga de la identificación del tipo de ficheros, así como, de su reconstrucción en tiempo real. Los resultados obtenidos son enviados luego a las herramientas de análisis para identificar comportamientos maliciosos en los mismos. En esta solución este servicio está configurado para observar todo el tráfico de entrada y salida que atraviesa el appliance, incluso el tráfico en entrada externo. Por las reglas de seguridad, el tráfico de entrada no sobrepasa el servidor cortafuego, con el objetivo de poder analizar todos los ficheros que intentan ingresar en la entidad.

1 Identificación de firma de malware conocida

2 Categoría de reputación asignada

3 Suma md5 de los ficheros creados en el sistema por el archivo analizado

4 Entradas en el registro de Windows creadas por el archivo analizado

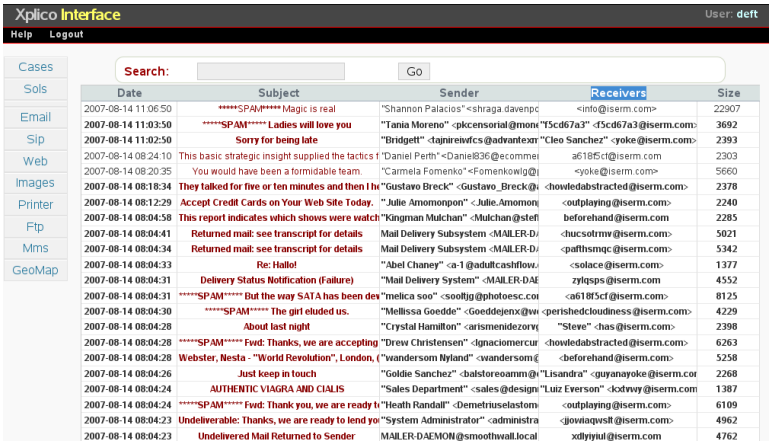


Figura 4. Reconstrucción de paquetes.

La solución brinda además varias interfaces para que los administradores puedan realizar análisis personalizados sobre los ficheros de tráfico capturados. Dichos análisis se realizan fundamentalmente con la herramienta de software libre Moloch. Este software se encarga de analizar todo el tráfico que circula por la red, con el objetivo de presentar interfaces de gestión detalladas que permitan desglosar dicho tráfico en estructuras lógicas para el análisis y la investigación de incidentes de seguridad. Cuenta con un gran número de filtros incorporados que facilitan las labores de los especialistas de seguridad, y permiten generar informes personalizados con la información obtenida como muestra la Figura 5.

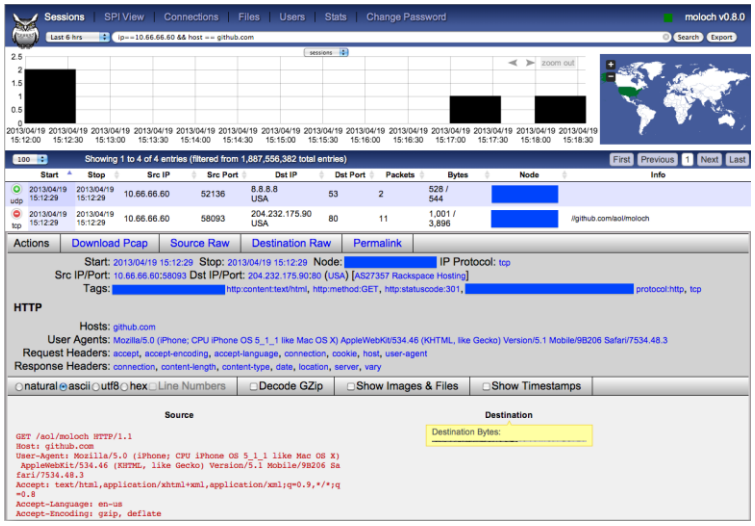


Figura5. Análisis de tráfico.

Servicio de monitorización de tráfico y análisis estadísticos

El appliance cuenta además con un servicio de monitorización de tráfico y análisis estadísticos, el cual se conforma a partir de la información almacenada por todas las herramientas que lo integran, ver Figura 6. Dicha información se obtiene y se presenta de forma tal, que facilite las tareas de análisis e

investigación, así como, la creación de informes resumen, según el estado de la seguridad de la infraestructura monitorizada. En esta funcionalidad se brinda información en cuanto a:

- Localización geográfica de los orígenes de las incidencias.
- Firmas de malware que han afectado a la infraestructura.
- Cantidad de ficheros analizados.
- Resumen de protocolos comprometidos en la infraestructura.
- Resumen de ficheros descargados.
- Resumen de incidencias por protocolos comunes (HTTP, SMTP, SSH, TLS, DNS).

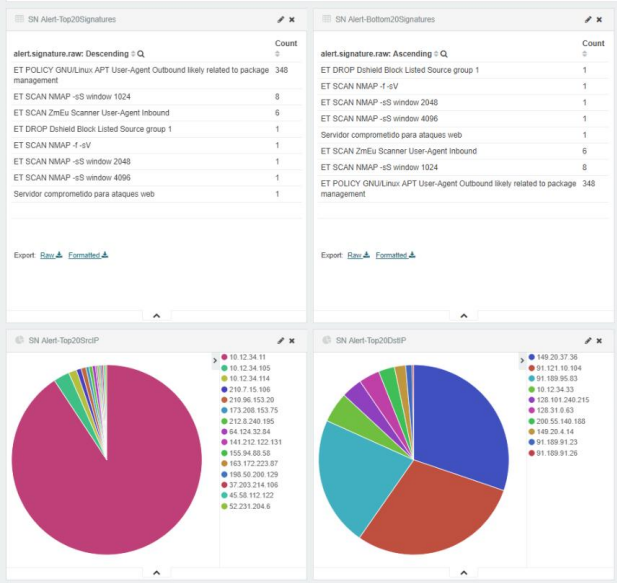


Figura. 6. Cuadros de Mando de Análisis.

CONCLUSIONES

La implementación de esta solución “appliance” permite cumplir con 3 fundamentos esenciales de la seguridad: prevenir, detectar y responder, a las amenazas informáticas que afectan hoy, gran parte de nuestras infraestructuras de redes. Recoge y organiza las labores de inspección de ficheros, servicios antivirus y antimalware, análisis de comportamiento, reconocimiento de patrones e identificación de reputación maliciosa con el objetivo de prevenir y detectar los ataques y vulnerabilidades que comprometen a los dispositivos informáticos. Además, emplea herramientas de bloqueo en tiempo de real, que garantizan la respuesta con mayor rapidez y precisión ante los incidentes de seguridad. De esta forma, se aumenta sustancialmente la protección de las redes informáticas. Esta solución facilita a los administradores de sistemas las tareas de análisis y monitoreo de sus infraestructuras. En adición, se colectan y envian automáticamente los incidentes informáticos que más afectan a un Centro de Comando y Control que cuenta con especialistas de seguridad altamente preparados. Estos especialistas realizan su análisis, modelación y correlación, con el objetivo de generar los patrones de respuesta que permitan minimizar su impacto en el resto de las entidades del país. Entre las expectativas de desarrollo de la solución se encuentra la integración con el resto de los servicios nacionales. Los servicios

nacionales se encargan de proveer soluciones de seguridad informática, fundamentalmente la incorporación como motor de análisis antivirus, del software "Segurmática Antivirus", así como, los grupos de trabajo del Centro de Seguridad del Ciber-espacio y la DOPS.

REFERENCIAS

[1] Buechler, M. C., Pingle, J. (2017). "The pfSense Book". Recuperado de: https://www.pfsense.org.

[2] Reid, K., Sanders, C. (2017). "Suricata Features". Recuperado de: https://suricata-ids.org/features/.

[3] Nolla, A. (2013). "Moloch: Capturing and Indexing Network Traffic in Realtime". Recuperado de: http://blog.alejandronolla.com/2013/04/06/moloch-capturing-and-indexing-network-traffic-in-realtime/.

[4] Guarneri, C., Tanasi, A., Bremer, J., Schloesser, M. (2017). Cuckoo Sandbox Book. Recuperado de: https://cuckoo.sh/docs/.

[5] Gianluca Costa, G., De Franceschi, A. (2017). "Xplico". Recuperado de: https://www.xplico.org.

[6] Huawei Technologies Co. (2017). "Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR1600&AR2200&AR3200&AR3600 series Enterprise Routers". Recuperado de: http://support.huawei.com/enterprise/en/doc/DOC1000009848/?idPath=7919710%7C21432787%7C7923148%7C22318718%7C6078839

[7] AlienVault, Inc. (2017). Recuperado de: http://reputation.alienvault.com/reputation.data.

[8] Emerging Threats. (2017). "Blockrules". Recuperado de: https://rules.emergingthreats.net/blockrules/.

[9] Blocklist. (2017). "Blocklist.de". Recuperado de: http://www.blocklist.de.

[10] CSIRT Gadgets Foundation. (2017). Recuperado de: http://csirtgadgets.org/collective-intelligence-framework/.

[11] AlienVault, Inc. (2017). Recuperado de: https://otx.alienvault.com/.