ANÁLISIS Y VALORACIÓN DE LOS DISPOSITIVOS DE SEGURIDAD PERIMETRAL NGFW Y WAF, ADQUIRIDOS E IMPLEMENTADOS POR EL MINISTERIO DE EDUCACIÓN NACIONAL DE COLOMBIA, QUE PERMITEN DETECCIÓN DE INTRUSOS y MALWARE.

LUIS ALEJANDRO PINILLA PERALTA

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERÍA
ESPECIALIZACIÓN DE SEGURIDAD INFORMÁTICA
BOGOTÁ, D.C.
2017

ANÁLISIS Y VALORACIÓN DE LOS DISPOSITIVOS DE SEGURIDAD PERIMETRAL NGFW Y WAF, ADQUIRIDOS E IMPLEMENTADOS POR EL MINISTERIO DE EDUCACIÓN NACIONAL DE COLOMBIA, QUE PERMITEN DETECCIÓN DE INTRUSOS y MALWARE.

LUIS ALEJANDRO PINILLA PERALTA

Proyecto de grado para optar al título de
Especialista en Seguridad Informática

Asesor
RICARDO HERRERA HERNÁNDEZ

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERÍA
ESPECIALIZACIÓN DE SEGURIDAD INFORMÁTICA
BOGOTÁ, D.C.
2017

Nota de Aceptación

Firma del presidente del Jurado

Firma del Jurado

Firma del Jurado

Bogotá D.C. 11 de diciembre de 2017

CONTENIDO

LISTA DE FIGURAS

pág.

Lista de Cuadros

pág.

Lista de Gráficas

pág.

Lista de Anexos

pág.

GLOSARIO

ADC *(Application delivery controller):* es un dispositivo de red que se encuentra ubicado estratégicamente entre el firewall y uno o más servidores de aplicaciones. El ADC gestiona el equilibrio de carga entre servidores y optimiza el rendimiento y la seguridad del usuario final para las aplicaciones empresariales[1].

ACTIVO: todo lo que tiene valor para la organización.

NOTA – Hay muchos tipos de activos y entre ellos se cuentan:

- la información;
- el software, como los programas informáticos;
- los físicos, como las computadoras;
- los servicios;
- las personas y sus calificaciones, conocimientos y experiencias; y
- los intangibles, como la reputación y la imagen[2].

AMENAZA: todo elemento o acción capaz de atentar contra la seguridad de la información[3].

ANÁLISIS HEURÍSTICO: detecta paquetes y patrones de tráfico anómalos como exploraciones de puertos y limpiezas de host[4].

APT (*Advanced Persistent Threat):* la amenaza persistente avanzada, es un conjunto de procesos informáticos sigilosos y continuos, a menudo orquestados por humanos, dirigidos a penetrar la seguridad informática de una entidad especifica utilizando software malicioso para explotar vulnerabilidades en los sistemas con fines delictivos[5].

---

[1] CITRIX. Citrix Glossary. [En línea], [consultado el 28 de noviembre de 2016]. Disponible en: https://www.citrix.com/glossary/. Traducción autor.

[2] ITU. Techniques for preventing web-based attacks. [En línea], [consultado el 28 de noviembre de 2016]. Disponible en: http://www.itu.int/itu-t/recommendations/rec.aspx?rec=12154. Traducción autor.

[3] SEGURIDAD INFORMÁTICA. Amenazas a la seguridad de la información. [En línea], [consultado el 23 de abril de 2016]. Disponible en: http://www.seguridadinformatica. unlu.edu.ar/?q=node/12

[4] PALO ALTO NETWORK. IPS para empresas. [En línea], [consultado el 23 de noviembre de 2016]. Disponible en: https://www.paloaltonetworks.es/products/features/ips.html

[5] VID INFO. 5 avanzadas persistentes amenazas APT. [En línea], [consultado el 23 de abril de 2016]. Disponible en: http://media.kaspersky.com/documents/business/brfwn/en/Advanced-persistent-threats-not-your-average-malware_Kaspersky-Endpoint-Control-white-paper.pdf. Traducción autor.

CAB *(CHANGE ADVISORY BOARD)*: Es un grupo de personas que dan soporte en la evaluación, priorización, autorización y programación de los cambios[6].

CMDB *(CONFIGURATION MANAGEMENT DATABASE)*: Es una base de datos utilizada para almacenar los registros de configuración a lo largo de su ciclo de vida[7].

CONFIDENCIALIDAD: la información llegue solamente a las personas autorizadas[8].

DEFACEMENT: es el método de modificar el contenido de un sitio web de tal manera que se convierte en vergonzoso para el propietario del sitio web[9].

DB (*Data Base*): Base de datos.

DISPONIBILIDAD: es la necesidad de asegurar que el propósito comercial del sistema puede ser accesible para aquellos que necesitan usarlo[10].

DMZ (*Demilitarized Zone*): es una sub-red que está detrás del Firewall, pero que tiene permisos de acceso desde la red pública. El público puede conectarse a los servicios en la DMZ, pero no puede acceder a la LAN. Normalmente se configura la DMZ para incluir cualquier host que deben ser expuestos a la WAN (tales como servidores web o de correo electrónico)[11].

DOS (*Deny of Service*): el ataque de denegación de servicio tiene como objetivo imposibilitar el acceso a los servicios y recursos de una organización durante un periodo definido en el tiempo[12].

---

[6] Registrada por la comunidad de la oficina de comercio del Gobierno de Inglaterra. ITIL FUNDAMENTOS DE ADMINISTRACIÓN DE SERVICIOS. Versión 5. United States: FoxIT, 2011, p.21.

[7] Registrada por la comunidad de la oficina de comercio del Gobierno de Inglaterra. ITIL FUNDAMENTOS DE ADMINISTRACIÓN DE SERVICIOS. Versión 5. United States: FoxIT, 2011, p.29.

[8] AMUTIO, Miguel. MAGERIT. Versión 3. España: Dirección General de Modernización Administrativa. 2012, p.9.

[9] SANS. Glossary of Security Terms. [En línea] [consultado el 23 de noviembre de 2016]. Disponible en: https://www.sans.org/security-resources/glossary-of-terms/. Traducción autor.

[10] SANS. Glossary of Security Terms. [En línea] [consultado el 28 de noviembre de 2016]. Disponible en: https://www.sans.org/security-resources/glossary-of-terms/. Traducción autor.

[11] CISCO, Configuring DMZ. [En línea] [consultado el 5 de marzo de 2016]. Disponible en: https://www.cisco.com/assets/sol/sb/isa500_emulator/help/guide/ad1681599.html. Traducción autor.

[12] DoS, DENIAL OF SERVICE. Ataque por denegación de servicio. [En línea], [consultado el 23 de abril de 2016]. Disponible en: http://es.ccm.net/contents/22-ataque-por-denegacion-de-servicio

FIRMAS: es un patrón distintivo en el tráfico de red que puede identificar un *malware* o exploit específico[13].

IDS (Intrusion Detection System): un sistema de detección de intrusiones (IDS) es una tecnología de seguridad de red construida para detectar explotaciones de vulnerabilidades contra una aplicación de destino o una computadora[14].

INTEGRIDAD: confirma el aseguramiento y precisión de los sistemas de información previniendo las modificaciones de usuarios o sistemas no autorizados[15].

INTRUSIÓN: se define como una secuencia de acciones relacionadas y realizadas por un atacante informático que resulta comprometiendo un sistema informático objetivo. Se asume que las acciones del intruso violan una política de seguridad[16].

IPS (Intrusion Prevention System): los Sistemas de Prevención de Intrusión (IPS) amplían las soluciones IDS añadiendo la capacidad de bloquear las amenazas además de detectarlas[17].

LAN (*Local Área Network*): una red residente en un lugar, como un solo edificio o campus[18].

MALWARE: término genérico para varios tipos diferentes de código malicioso la cual parece desempeñar una función útil o deseable, pero que en realidad obtiene acceso no autorizado a los recursos del sistema o engaña a un usuario para que ejecute otra lógica malintencionada[19].

MEN: Ministerio de Educación Nacional.

---

[13] SANS. Glossary of Security Terms. [En línea] [consultado el 28 de noviembre de 2016]. Disponible en: https://www.sans.org/security-resources/glossary-of-terms/. Traducción autor.

[14] PALO ALTO NETWORK. Intrusion Detection System - IDS technology and deployment. [En línea], [consultado el 23 de noviembre de 2016]. Disponible en: https://www.paloaltonetworks.com/documentation/glossary/what-is-an-intrusion-detection-system-ids. Traducción autor.

[15] SHON, Harris. CISSP. 6 ed. United States: American Express, 2013, p.23. Traducción autor.

[16] KRUEGEL, Christopher. VALEUR, Fredrik. VIGNA, Giovanni. Intrusion Detection and Correlation, Volumen 14, Springer US, 2005, p.17. Traducción autor.

[17] PALO ALTO NETWORK. Intrusion Detection System - IDS technology and deployment. [En línea], [consultado el 23 de noviembre de 2016]. Disponible en: https://www.paloaltonetworks.com/documentation/glossary/what-is-an-intrusion-detection-system-ids. Traducción autor.

[18] CISCO, Glossary, [En línea] [consultado el 28 de noviembre de 2016]. Disponible en: http://www.cisco.com/c/en/us/td/docs/security/asa/asa80/configuration/guide/conf_gd/glossary.html#wp1022456. Traducción autor.

[19] SANS. Glossary of Security Terms. [En línea] [consultado el 23 de noviembre de 2016]. Disponible en: https://www.sans.org/security-resources/glossary-of-terms/. Traducción autor.

PHISHING: el uso de medios basados en computadoras engañosas para suplantar a las personas para que divulguen información personal sensible a través de un mensaje de correo electrónico cuidadosamente elaborado[20].

RANSOMWARE: software malicioso creado por un hacker que restringe el acceso al sistema que infecta, y que permite al hacker pedir un rescate al usuario a cambio de eliminar esta restricción. Algunos tipos de ransomware podrían cifrar los archivos en el disco duro del sistema, mientras que otros podrían simplemente bloquear el sistema y mostrar mensajes instando al usuario a pagar[21].

RFC (*Request for change*): es una solicitud de cambio a cualquier ítem de configuración (CI) dentro de una. Un RFC incluye detalles del cambio propuesto, y puede ser registrado en papel o electrónicamente[22]**.**

RIESGO: estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización[23].

NGFW (*Next Generation Firewall*): son Firewall de inspección de paquetes profundos que se mueven más allá de la inspección y bloqueo de puertos / protocolos para agregar inspección a nivel de aplicación y prevención de intrusiones[24].

SSID (*Service Set identifier)*: es un identificador único que los dispositivos de red inalámbrica para establecer y mantener la conectividad inalámbrica. Múltiples puntos de acceso / puentes en una red o subred pueden utilizar el mismo SSID[25]**.**

VALORACIÓN: una serie de actividades que determinan hasta qué punto un control de seguridad se implementó correctamente, operando según lo previsto y produciendo un resultado deseado con respecto al cumplimiento de los requisitos de seguridad de un el sistema[26].

---

[20] MATT, Walker, CEH. 2 ed. United Sates: American Express, 2014, p.403. Traducción autor.

[21] McAfee. Glosario. [En línea] [consultado el 23 de noviembre de 2016]. Disponible en: https://home.mcafee.com/virusinfo/glossary#H.

[22] WSP-CONSULTING. Request for Change (RFC). [En línea] [consultado el 29 de noviembre de 2016] Disponible en: https://wsp-consulting.de/SM_help/content/glossary/request_for_change_rfc.htm. Traducción autor.

[23] AMUTIO, Miguel. MAGERIT. Versión 3. España: Dirección General de Modernización Administrativa. 2012. p.9.

[24] GARTNER, IT Glossary. [En línea] [consultado el 29 de noviembre de 2016] Disponible en: http://www.gartner.com/it-glossary/next-generation-firewalls-ngfws. Traducción autor.

[25] CISCO, Chapter: Configuring SSIDs. [En línea] [consultado el 5 de marzo de 2016]. Disponible en:http://www.cisco.com/c/en/us/td/docs/wireless/access_point/1300/12-2_15_JA/configuration/guide/o13ssid.html. Traducción autor.

[26] MATT, Walker, CEH. 2 ed. United Sates: American Express, 2014, p.386. Traducción autor.

VLAN (*Virtual LAN*): es un grupo de dispositivos en uno o más LANs que están configurados para comunicarse entre sí, como si estuvieran conectados al mismo cable, cuando en realidad se encuentran en un número de diferentes segmentos de la LAN. Debido a que las VLAN se basan en conexiones lógicas en vez de físicas, son extremadamente flexibles[27].

WAF (*Web Aplication Firewall*): es un dispositivo que tiene características para filtrar ataques de aplicaciones web por medio de un conjunto de reglas para una conexión HTTP. En general, estas normas se refieren a los ataques comunes tales *como cross-site scripting* (XSS) y la inyección de SQL . Mediante la personalización de las reglas para su aplicación, muchos ataques pueden ser identificados y bloqueados. El esfuerzo para llevar a cabo esta personalización puede ser importante y debe ser mantenido a medida que se evolucionan las aplicaciones[28].

UTM (*Unified Threat Management*): la tecnología de administración unificada de amenazas (UTM), proporciona protección completa para simplificar la administración de la seguridad, sin reducir la velocidad de la red, estos dispositivos comprenden los siguientes modulo antivirus de puerta de enlace, antimalware, antispam, prevención de intrusiones, filtrado de contenido/URL, SSL VPN y capacidades de control de aplicación en un solo paquete[29].

VULNERABILIDAD: debilidad de un sistema que permite a un atacante violar la confidencialidad, integridad, disponibilidad, control de acceso y consistencia del sistema o de sus datos y aplicaciones[30].

---

[27] CISCO, Chapter: Understanding and Configuring VLANs. [En línea] [consultado el 5 de marzo de 2016]. Disponible en: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/25ew/configuration/guide/conf/vlans.html. Traducción autor.

[28] OWASP. Aplicación Firewall. [En línea], [consultado el 23 de abril de 2016]. Disponible en: https://www.owasp.org/index.php/Web_Application_Firewall&prev=search. Traducción autor.

[29] SONICWALL. Soluciones de administración unificada. [En línea], [consultado el 23 de abril de 2016]. Disponible en: http://www.sonicwall.com/mx-es/solutions/unified-threat-management/.

[30] ALEGSA.COM. Definición de vulnerabilidad. [En línea], [consultado el 23 de abril de 2016]. Disponible en: http://www.alegsa.com.ar/Dic/vulnerabilidad.php.

INTRODUCCIÓN

El Ministerio de Educación Nacional, en adelante MEN, es el organismo que tiene como misión garantizar el derecho a la educación con criterios de equidad, calidad y efectividad en todo el territorio Colombiano; para ello cuenta con una infraestructura tecnológica, que tiene más de 200 aplicaciones y 2 centros alternos, la cual debe ser protegida de múltiples amenazas entre las que se encuentran: *malware, defacement, ransomware,* APT (*Advanced Persistent Threat)**,** phishing*, ataques informáticos, entre otros. Estas amenazas evolucionan de manera exponencial, por lo que es de vital importancia valorar y analizar los dispositivos de seguridad NGFW y WAF adquiridos e implementados sobre la infraestructura perimetral, los cuales requieren de monitoreo y afinamiento para minimizar la materialización de amenazas preservando la integridad, confidencialidad y disponibilidad de los activos del MEN.

1. TITULO

ANÁLISIS Y VALORACIÓN DE LOS DISPOSITIVOS DE SEGURIDAD PERIMETRAL NGFW Y WAF, ADQUIRIDOS E IMPLEMENTADOS POR EL MINISTERIO DE EDUCACIÓN NACIONAL DE COLOMBIA, QUE PERMITEN DETECCIÓN DE INTRUSOS y MALWARE.

2. FORMULACIÓN DEL PROBLEMA

Actualmente la gran mayoría de las empresas, entre ellas el MEN, adquieren dispositivos y software de seguridad realizando una configuración por defecto sin realizar un análisis, valoración o restricciones sobre los mismos, disminuyendo la capacidad de contención de ataques informáticos o *malware*, afectando así la disponibilidad, integridad y confidencialidad de la infraestructura tecnológica del MEN, lo que lleva a plantearnos la siguiente pregunta de investigación:

¿Cuáles son los requisitos, procesos y parametrización necesarios para que los dispositivos de seguridad NGFW y WAF proporcionen una detección y prevención de ataques informáticos y *malware* a nivel perimetral de una manera eficaz y óptima?

3. JUSTIFICACIÓN

El crecimiento y evolución de las amenazas informáticas son de gran preocupación para el MEN, por lo tanto, como una medida de control y basado en las buenas prácticas de seguridad, la entidad ha adquirido los dispositivos de seguridad NGFW y WAF, los cuales requieren ser valorados, analizados y ajustados constantemente para aumentar la contención y prevención de ataques informáticos o *malware*.

4. OBJETIVOS

4.1 OBJETIVO GENERAL

Realizar valoración, análisis y afinamiento de los dispositivos NGFW y WAF del MEN, el cual detectan los diferentes ataques informáticos o *malware*, con la finalidad de activar los controles correctivos y/o preventivos, permitiendo preservar la integridad, disponibilidad y confidencialidad de los activos de información del MEN.

4.2. OBJETIVOS ESPECÍFICOS

- Analizar y estudiar la arquitectura de red, zonas, direccionamiento y permisos de firewall, permitiendo conocer el tipo de tráfico y accesos entre las diferentes zonas y así dimensionar las amenazas internas o externas a los que están expuestos.

- Evaluar los dispositivos de seguridad NGFW y WAF con el objetivo de conocer sus fortalezas y debilidades, para así, tener una línea base de su alcance según sus características y en caso de tener limitantes proporcionar recomendaciones al MEN, para la adquisición o renovación de sus productos de seguridad perimetral NGFW y/o WAF.

- Describir el flujo de aprobación formal para el afinamiento de los dispositivos, con el objetivo de preservar la disponibilidad de los activos de información minimizando el riesgo de bloquear funcionalidades de los servicios y aplicativos del MEN.

- Conocer e identificar las aplicaciones críticas del MEN de acuerdo a lo definido por la entidad, con la finalidad de priorizar los eventos o alarmas detectados en los dispositivos NGFW y WAF.

- Realizar y analizar el resultado del escaneo de vulnerabilidades de los servidores del MEN, con el objetivo de identificar las posibles amenazas en los registros de logs de los dispositivos NGFW y WAF que se pueden materializar, de acuerdo a las vulnerabilidades ya identificadas, permitiendo activar controles de manera temprana.

- Analizar los eventos y alarmas detectadas por los dispositivos NGFW y WAF de amenazas o *malware*, con el objetivo de solicitar formalmente controles correctivos y/o preventivos.

- Dar a conocer la dinámica de afinamiento tomando una muestra del análisis de las gráficas estadísticas mensuales de la categoría del top de amenazas con base a los eventos y alarmas detectadas por el dispositivo NGFW.

- Ponderar y analizar el resultado de las gráficas mensuales de la categoría de amenazas y *malware* bloqueados, el cual permitirá observar el nivel de contención para el período de tiempo que abarca este proyecto.

- De presentarse un incidente de seguridad, se realizará la respectiva inspección y análisis sobre los dispositivos NGFW y WAF, con el objetivo de identificar si se activó una firma derivado del ataque informático, de ser positivo este análisis se solicitará formalmente para la activación de bloqueo de estas firmas.

5. TIPOS DE INVESTIGACIÓN

Este proyecto abarca los tipos de investigación descriptivo y correlacional, debido a que busca describir y detallar las características de los dispositivos de seguridad perimetral NGFW y WAF, con la finalidad de realizar un afinamiento de configuración y el análisis de logs y gráficas estadísticas, el cual está fundamentado en un estudio de correlación y análisis de eventos, amenazas, ataques informáticos y *malware*.

6. HIPÓTESIS

6.1 HIPÓTESIS GENERAL

Al llevar a cabo un análisis permanente de los eventos y alarmas, evidenciadas en los logs y diagramas estadísticos generados sobre los dispositivos NGFW y WAF, permitirá proponer controles correctivos y/o preventivos sobre las amenazas detectadas sobre los mismos, salvaguardando los activos y preservando la integridad, confidencialidad y disponibilidad del MEN.

6.2 HIPÓTESIS NULA

Al llevar a cabo un análisis permanente de los eventos y alarmas, evidenciadas en los logs y diagramas estadísticos generados sobre los dispositivos NGFW y WAF, no permitirá proponer controles correctivos y/o preventivos sobre las amenazas detectadas sobre los mismos, salvaguardando los activos y preservando la integridad, confidencialidad y disponibilidad del MEN.

7. VARIABLES

7.1 VARIABLE INDEPENDIENTE

- Valorización de dispositivos de seguridad.
- *Malware*.
- Ataques informáticos.
- Incidente.
- Herramientas de seguridad.

7.2 VARIABLE DEPENDIENTE

- Controles.
- NGFW.
- WAF.

8. MARCO TEÓRICO

Un Sistema de Detección de Intrusos o IDS (*Intrusion Detection System*), es una herramienta centralizada de seguridad de software y/o hardware encargada de examinar el tráfico a nivel de red o host para identificar y alarmar los intentos de intrusión o *malware* con la ayuda de patrones específicos llamados firmas o por análisis heurístico.

Como describe Shon Harris en el libro de CISSP:

> La detección y la protección de una empresa a nivel de seguridad informática, debe tener presente el aumento y variedad de vectores de ataque y *malware*, la cual requiere algo más que una instalación de software antivirus o spyware, sino que al igual que las distintas áreas de TI, es necesario en el marco de seguridad tener presente los controles a nivel administrativo, físico y técnico, la cual requiere de una planeación, implementación, seguimiento, mantenimiento y mejora continua[31].

De acuerdo a lo citado anteriormente para el mantenimiento y aseguramiento continuo a nivel de seguridad informática es indispensable enfocar los esfuerzos en los controles preventivos tales como el análisis del IDS, ya que a nivel personal y profesional, el ejercicio de realizar el análisis del IDS de manera profunda y periódica se ha dejado de lado en la gran mayoría de las empresas, debido a que solo se revisa este módulo cuando se materializa un incidente de seguridad para rastrear e identificar el tipo de ataque y vulnerabilidad explotada para posteriormente aplicar controles correctivos.

Para realizar un correcto análisis de sistemas de detección de intrusos es necesario estudiar y entender los tipos de amenazas, ataques y consecuencias que generan, lo que permite enfocar el análisis del IDS revisando y correlacionando cierto tipo de patrones utilizados por los atacantes informáticos.

En el cuadro 1 los tipos de amenazas y ataques que buscan de manera fraudulenta la obtención, robo, difamación y/o pérdida de información. Esto, basado en el RFC 4949 que describe las diferentes acciones que pueden llevar a cabo estas amenazas con sus respectivas consecuencias.

[31] SHON, Harris. CISSP. 6 ed. United States: American Express, 2013, p.1383. Traducción autor.

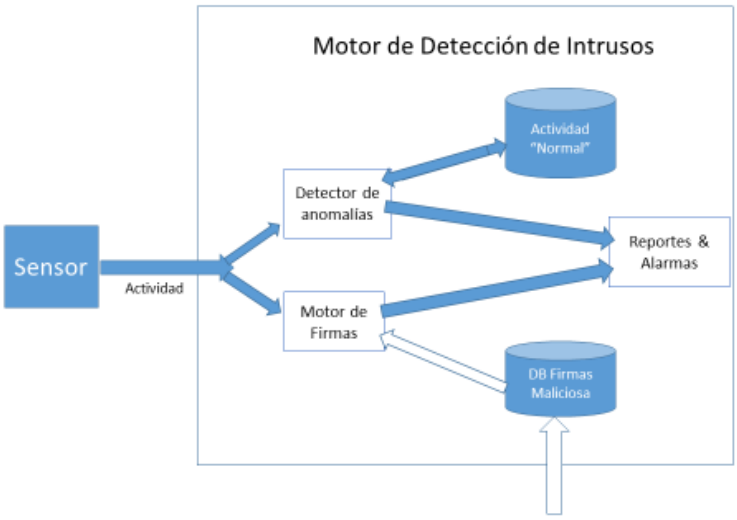
Cuadro 1. Descripción de amenazas y modalidades de ataques informáticos

Consecuencia de la amenaza	Tipos de amenaza (atacante)
Divulgación no autorizada: Circunstancia o evento que se presenta cuando el atacante tiene acceso a información y la comparte de manera no autorizada por el propietario.	**Exposición:** Información sensible está expuesta y a disposición del atacante informático. **Intercepción:** La información es interceptada por el atacante a través de medios de comunicación LAN, WIFI o WAN. **Deducción:** Este tipo de amenaza ocurre cuando el atacante o intruso realiza observación de los patrones de tráfico o al percatarse de que existe un patrón deducible en los controles de seguridad o de que no existen políticas de controles de acceso, obtiene acceso a información confidencial. **Intrusión:** Cuando el atacante informático (hack) burla la protección de seguridad teniendo acceso a información confidencial y sensible de manera no autorizada.
Fraude: Circunstancia o evento donde el atacante engaña enviando información falsa que hace pasar por verdadera.	**Disfraz:** El atacante adquiere acceso no autorizado y desarrolla un acto malicioso haciéndose pasar por un usuario legítimo. **Falsificación:** Sucede cuando el atacante engaña utilizando datos falsos a una entidad. **Negación:** Sucede cuando el atacante o grupo delictivo engaña a una entidad y niega la responsabilidad de los actos.
Interrupción: Circunstancia o evento que interrumpe o impide el correcto funcionamiento del sistema de información, afectando la disponibilidad e integridad de este.	**Indisponibilidad:** Ocurre a causa de la materialización de un *malware* o daño físico de la infraestructura física provocando indisponibilidad, sobre esta. **Alteración del sistema:** Es un ataque a la integridad del sistema la cual busca alterar el normal comportamiento del programa con fines delictivos o fraudulentos. **Obstrucción:** Es un ataque que impide o altera la comunicación con el objetivo de causar indisponibilidad del servicio.
Usurpación: Circunstancia o evento en el cual el atacante informático toma acceso y/o control del sistema de información de manera no autorizada con fines delictivos, afectando la integridad de este.	**Apropiación indebida:** El atacante o grupo delictivo obtiene el control de un sistema de información o bloquea el acceso del mismo como por ejemplo un ataque de DoS. **Uso indebido:** Un atacante informático accede a un sistema de seguridad y lo altera para que no sea detectado posteriormente el ataque.
Fuente: STALLINGS, William Lawrie brown. Computer Security Principles and practices. (Base RFC7474). p 18. Traducción autor.	

8.1 ESTRUCTURA Y ANÁLISIS DE ALARMAS DEL IDS/IPS

Para entender la estructura básica del IDS y su funcionamiento, en la figura 1 se ilustra cada uno de sus componentes:

Figura 1. Componentes de IDS



Fuente: CROTHERS, Tim. Implementing Intrusion Detection System. Indianapolis, Wiley publishing, Inc., 2003, p.10.

El origen de la información generada ya sea por PCs, *smartphones*, servidores, aplicaciones entre otros, suministran datos que están compuestos por paquetes, los cuales son escaneados en el trayecto de comunicación por medio de un motor de detector de intrusos como se observa en la figura 1. El motor de detección de intrusos se compone inicialmente por un **sensor** que identifica el trafico normal "benévolo" o de tipo *malware* con la ayuda del **detector de anomalías** y **motor de Firmas**. El módulo de **detector de anomalías** tiene la tarea de capturar el tráfico sospechoso y almacenarlo en la base de datos **actividad "normal"** y en este punto se lleva una traza del tráfico con el objetivo de detectar un ataque informático para posteriormente enviarlo al módulo de **reportes y alarmas**.
El módulo de **motor de firmas** consiste en escanear y comparar el tráfico en busca de patrones ya identificados y definidos como maliciosos, los cuales llamaremos "firmas" que son almacenadas en una base de datos **DB actividad maliciosa**, cabe indicar que la efectividad de este módulo consiste en que su base de datos continuamente se esté actualizando con los últimos patrones anómalos conocidos, con el objetivo de detectar las amenazas más recientes.

El módulo de **reportes y alarmas** se alojan todos los registros de la actividad considerada como *malware* categorizada por severidad, estas alarmas requieren ser analizadas por una persona especializada en seguridad informática, con el fin de activar los controles respectivos para salvaguardar a la empresa de atacantes informáticos y/o propagación de *malware* al interior de la misma.

Para analizar los resultados de un sistema de detección de intrusos es necesario conocer los diferentes tipos de filtros o reportes que se puede realizar en el módulo de **reportes y alarmas** que facilitan significativamente la detección de intrusos o *malware*. A continuación, se explica cada uno de ellos:

Reportes: Son informes consolidados que aportan un panorama global del resultado de los logs partiendo de los paquetes de detección de intrusos.

Visualización: Son las herramientas de IDS que permiten visualizar por medio de un tablero de control ya sea en tiempo real o por períodos de tiempo definidos por el analista que facilitan la clasificación del tráfico de tal manera que son de mucha utilidad para tomar decisiones en cuanto al bloqueo de cierto tipo de tráfico.

Correlación: Es una característica de los IDS que permite establecer relaciones lógicas entre eventos independientes ayudando a la reducción de falsas alarmas y normalmente estos eventos son categorizados por la severidad del ataque facilitando la comprensión.

Evaluación de vulnerabilidad: Hace referencia a la correlación de amenazas detectadas por el IDS contra las vulnerabilidades identificadas al interior de una empresa u organización, permitiendo conocer la gravedad y las consecuencias de los ataques detectados por el IDS.

Minería de datos: Comprende el análisis estadístico de los datos existentes que en conjunto permiten detectar patrones que no son identificables de manera aislada[32].

Como se explicó anteriormente un *Intrusion Detection System* (IDS), es una tecnología de seguridad informática construida para la detección de amenazas ya sea hacia un ordenador o aplicación de destino. Los *Intrusion Prevention System* (IPS) es una solución extendida de los IDS los cuales **añaden capacidad para bloquear amenazas además de detectarlas** y se han convertido en la opción dominante para el despliegue de tecnologías en conjunto denominadas IDS/IPS.

Como se describió anteriormente, el IDS es un dispositivo de escucha. El IDS escanea el tráfico y reporta sus resultados a un dispositivo o servidor, pero

[32] CROTHERS, Tim. Implementing Intrusion Detection System. Indianápolis, Wiley publishing, Inc., 2003, p.10-11. Traducción autor.

automáticamente no puede tomar medidas para prevenir o bloquear un ataque detectado sobre la solución IDS.

En el siguiente cuadro 2 resume las diferencias que existen entre los sistemas IDS e IPS.[33]

Cuadro 2. Diferencias de las tecnologías IPS e IDS

Característica	Sistemas de prevención de intrusos(IPS)	Sistema de detección de intrusos(IDS)
Lugar en la infraestructura	Debe atravesar el dispositivo para su comunicación (inline).	Se encuentra afuera de la línea de comunicación (out-of-band).
Tipo de sistema	Activo (monitorea & automáticamente detiene) y/o pasivo.	Pasivo (monitorea & notifica).
Mecanismos de detección	• Estadísticas basadas en detecciones anómalas. • Detección de firmas: explotadas o vulneradas.	Detección firmas.
Fuente: PALO ALTO NETWORK. Intrusion Detection System - IDS technology and deployment. [En línea], [consultado el 23 de noviembre de 2016]. Disponible en: https://www.paloaltonetworks.com/documentation/glossary/what-is-an-intrusion-detection-system-ids. Traducción autor.		

8.2 MÉTODOS DE GESTIÓN NIDS Y HIDS

Actualmente existen dos métodos de gestión de detección de intrusos el primero a nivel de red (NIDS) y el segundo a nivel de host (HIDS), a continuación, se explicarán cada uno de ellos:

NIDS (Network IDS): Es un sistema de detección de intrusos ubicado en la red; normalmente son dispositivos que escanean y discriminan el tráfico en tiempo real en busca de tráfico anómalo, tales como DoS, escaneo de puertos, ataques informáticos entre otros.

HIDS (Host IDS): Es un sistema de detección de intrusos a nivel de host instalados en la maquina final, el cual reporta el tráfico a un servidor centralizado analizando el tráfico en busca de comportamiento anómalo[34].

[33] PALO ALTO NETWORK. Intrusion Detection System - IDS technology and deployment. [En línea], [consultado el 23 de noviembre de 2016]. Disponible en: https://www.paloaltonetworks.com/documentation/glossary/what-is-an-intrusion-detection-system-ids. Traducción autor.

[34] CROTHERS, Tim. Implementing Intrusion Detection System. Indianápolis, Wiley publishing, Inc., 2003, p.12. Traducción autor.

Es importante resaltar que los NIDS son más populares y utilizados que los HIDS debido al costo, mayor rango de detección y facilita la trazabilidad. Cabe aclarar que los NGFW y WAF hacen parte del grupo de NIDS elementos de investigación de este proyecto.

8.3 MARCO TEÓRICO DE REFERENCIA MEN

En este ítem se busca dar a conocer la misión y visión del MEN permitiendo entender de manera general los objetivos y propósito de la entidad; de la cual se pretende salvaguardar de ataques informáticos y *malware* apoyados en el análisis del sistema de detección y prevención de intrusos:

8.3.1 Misión: Lograr una EDUCACIÓN DE CALIDAD, que forme mejores seres humanos, ciudadanos con valores éticos, competentes, respetuosos de lo público, que ejercen los derechos humanos, cumplen con sus deberes y conviven en paz. Una educación que genere oportunidades legítimas de progreso y prosperidad para ellos y para el país.

Lograr una educación competitiva, pertinente, que contribuya a cerrar brechas de inequidad y en la que participa toda la sociedad.

8.3.2 Visión: En el 2018, el Ministerio de Educación es la entidad líder del Gobierno Nacional, con reconocimiento internacional, que atrae a los mejores talentos y está 100% orientada a hacer de Colombia el país más educado de América Latina en el 2025. Es una entidad innovadora, creativa, eficiente, generadora de investigación y conocimiento para el país y para el mundo. Es una entidad ejemplar por su ejecución[35].

8.3.3 Dispositivos y herramientas de seguridad del MEN. Es importante conocer los dispositivos y herramientas de seguridad con los que cuenta el MEN, de tal manera que permita utilizar contramedidas adecuadas y más efectivas de acuerdo al ataque informático o malware, ya sea a nivel WEB, phishing, spam, virus, defacement, inyección de SQL, Cross site scripting entre otros, a continuación, se listan los dispositivos o herramientas de seguridad:

[35] MINISTERIO DE EDUCACIÓN. Lineamientos técnicos y administrativos. [En línea], [consultado el 23 de abril de 2016]. Disponible en: http://www.mineducacion.gov.co/1759/w3-article-89266.html

Software Seguridad:

- Antivirus Kaspersky.
- Antivirus ClamAV.
- Script Defacement.

Dispositivos Seguridad:

- NGFW: Palo Alto, Dell Sonicwall, Cisco ASA.
- Anti-Spam: IronPort Mail.
- Content Filter: IronPort Web.
- WAF NetScaler.

Los dispositivos anteriormente mencionados se encuentran distribuidos en los dos centros de datos que cuenta el MEN, la sede del CAN y la sede de DIVEO, para mayor detalle del diagrama de red y su distribución remitirse al numeral 10 Arquitectura.

8.4 DISPOSITIVOS NGFW y WAF

El MEN actualmente cuenta con cuatro NGFW Palo Alto Netwoks en alta disponibilidad con las siguientes referencias:

- 2 PA-3020 en alta disponibilidad en sede CAN
- 2 PA-3050 en alta disponibilidad para sede DIVEO.

A nivel de WAF cuenta con 4 dispositivos la siguiente referencia en alta disponibilidad:

- 4 MPX-5650 en alta disponibilidad para la sede DIVEO.

A continuación, se realizará una breve descripción con las características y cualidades de los dispositivos NGFW y WAF, tomando como referencia la página de cada fabricante.

8.4.1 NGFW Palo Alto Network. Los ataques avanzados en la red utilizan una combinación de vectores tales como: *exploits*, desbordamientos de búfer, APTs, virus, spyware, entre otros. Los NGFW están en la capacidad de detectar y contener estos ataques por medio de firmas, heurísticas y detección de anomalías estadísticas. Además, ofrecen un rendimiento IPS predecible a través de aceleración de hardware, un formato de firma uniforme y una arquitectura de software de paso único.

8.4.1.1 Prevención de amenazas. La combinación de Content-IDTM y WildFireTM proporciona protección contra amenazas conocidas y desconocidas. Content-ID limita la transferencia de datos no autorizados y detecta y bloquea una amplia gama de amenazas. WildFire identifica *malware* desconocido, explotaciones de día cero y amenazas persistentes avanzadas mediante análisis estático y dinámico en un entorno virtual escalable y distribuye automáticamente protecciones actualizadas globalmente en tiempo casi real.

El módulo de Wildfire clasifica las firmas en tres categorías (*malware*, *greyware* y *benign*), la cual se explican a continuación:

Malware: Los archivos clasificados como *malware* son maliciosos en intención o naturaleza y pueden representar una amenaza para la seguridad. Los programas maliciosos pueden incluir virus, gusanos, troyanos, herramientas de acceso remoto (RAT), rootkits y botnets. Para los archivos identificados como *malware*, la nube WildFire genera y distribuye una firma para evitar la exposición futura.

Greyware: Los archivos clasificados como *grayware* no representan una amenaza directa a la seguridad, pero pueden mostrar un comportamiento de otro modo invasivo. *Grayware* puede incluir, *adware*, *spyware* y objetos de ayuda del navegador (BHOs).

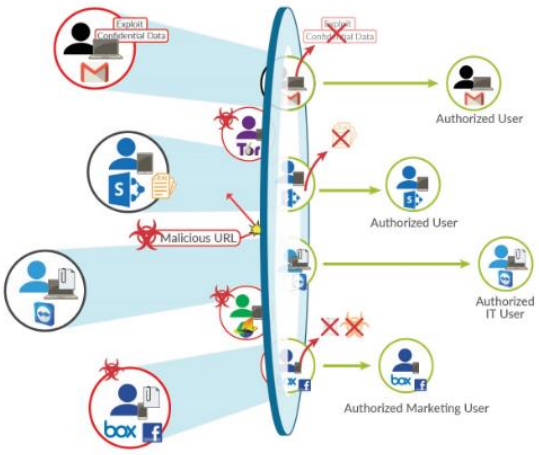
Benign: Los archivos categorizados como benignos son seguros y no presentan comportamiento malicioso[36].

Los NGFW Palo Alto esta conpuesto por varios módulos de seguridad enfocados en evitar amenazas cibernéticas avanzadas y desconocidas, apoyados con un análisis local y actualizándose continuamente con una base de datos en la nube propiedad de la marca[37].

La figura 2 es una representación del escaneo que se realiza a nivel de aplicación donde, al atravesar la inspección a nivel de aplicación en los NGFW Palo Alto, bloqueando el tráfico malicioso.

[36] PALO ALTO NETWORK. IPS. [En línea], [consultado el 25 de noviembre de 2016]. Disponible en:https://www.paloaltonetworks.com/products/secure-the-network/next-generation-firewall. Traducción autor.
[37] PALO ALTO NETWORK. IPS. [En línea], [consultado el 25 de noviembre de 2016]. Disponible en:https://www.paloaltonetworks.com/products/secure-the-network/next-generation-firewall Traducción autor.

Figura 2. Escaneo a nivel de aplicaciones



Fuente: PALO ALTO NETWORK. IPS. [En línea], [consultado el 25 de noviembre de 2016]. Disponible en: https://www.paloaltonetworks.com/products/secure-the-network/next-generation-firewall

En el siguiente numeral se describirá los módulos de seguridad del dispositivo NGFW a los que se realizará afinamiento.

8.4.1.2 Bloqueo de amenazas conocidas compuesto por los modulos IPS, Antivirus de red y Anti-spyware, donde cada módulo tiene un motor de exploración de tráfico, el cual permite proteger la red de una amplia gama de amenazas.
El sistema de prevención de intrusiones (IPS) presenta bloqueos de amenazas en la capa de aplicación y de red, tales como, desbordamientos de búfer, ataques DoS y exploraciones de puertos entre otros. La protección anti-virus y anti-spyware bloquea millones de variantes de *malware*, así como cualquier tráfico generado por software malicioso con virus, gusanos, troyanos o *malware* oculto, también tiene la capacidad de inspeccionar los archivos comprimidos o tráfico web (HTTP / HTTPS comprimidos).[38].

A continuación, se explicarán los módulos de protección con mayor detalle:

Protección anti-virus: Este módulo usa un motor de inspección de tráfico en busca de virus, gusanos y troyanos, sin afectar significativamente el rendimiento del dispositivo. El módulo de anti-virus busca una gran variedad de *malware* en

[38] PALO ALTO NETWORK. Next-Generation Firewall Overview. [En línea], [consultado el 23 de noviembre de 2016]. Disponible en: http://www.paloalto-firewalls.com/wp-content/uploads/2013/03/Palo-Alto-Firewall-Overview.pdf. Traducción autor.

distintos archivos tales como, ejecutables, archivos PDF, HTML, JavaScript, y archivos comprimidos entre otros. Adicionalmente si se ha activado el descifrado en el firewall, el módulo anti-virus también permite el análisis de contenido en este tipo de tráfico.

Dentro de los protocolos que puede escanear el módulo de anti-virus se encuentran SMTP, IMAP y POP3, HTTP, FTP y SMB, al detectar algún paquete con *malware* realiza la respectiva acción de contención de acuerdo con la parametrización de este módulo[39].

Protección anti-spyware: El módulo de anti-spyware ayuda a bloquear el spyware en los hosts comprometidos, ya que el NGFW permite detectar y bloquear el tráfico malicioso en el momento que el host infectado envía solicitudes hacia servidores externos (atacante), adicionalmente se puede personalizar este módulo a nivel de zonas, es decir se pueden definir zonas confiables y no confiables activando este módulo en las zonas no confiables como por ejemplo la zona WAN que da acceso a internet.

La protección anti-spyware, puede habilitar la acción Sinkholing de DNS para forzar el bloqueo de una respuesta a una consulta DNS de un dominio malicioso conocido, esta función ayuda a identificar los hosts infectados en una red protegida mediante DNS.

Los hosts infectados por el tráfico pueden ser identificados fácilmente en los registros de tráfico de amenazas, debido a que los equipos que tratarán de comunicarse a los DNS maliciosos serán redirigidos a la IP sinkhole[40].

Protección Amenazas: El módulo de protección contra amenazas permite bloquear ataques del tipo *buffer overflow*, ejecución de código (*exploits*), ataques de diccionario y otros intentos para aprovechar las vulnerabilidades internas de la entidad o empresa.

Los perfiles de anti-spyware ayudan a identificar hosts infectados cuando el tráfico es saliente, por ejemplo, desde un computador comprometido que trate de enviar información hacia dominios que se encuentran definidos como maliciosos en la internet[41].

---

[39] PALO ALTO NETWORK. Antivirus Profiles. [En línea], [consultado el 23 de noviembre de 2016]. Disponible en: https://www.paloaltonetworks.com/documentation/70/pan-os/pan-os/policy/antivirus-profiles. Traducción autor.

[40] PALO ALTO NETWORK. Antivirus Profiles. [En línea], [consultado el 23 de noviembre de 2016]. Disponible en: https://www.paloaltonetworks.com/documentation/61/pan-os/pan-os/policy/anti-spyware-profiles . Traducción autor.

[41] PALO ALTO NETWORK. Antivirus Profiles. [En línea], [consultado el 23 de noviembre de 2016]. Disponible en: https://www.paloaltonetworks.com/documentation/70/pan-os/pan-os/policy/antivirus-profiles. Traducción autor.

El perfil por defecto es proteger a los clientes y servidores de todas las amenazas con severidad *critical*, *high* y *medium*, adicionalmente también se pueden crear excepciones de detectar firmas como falsos positivos.

8.4.1.3 Acciones de protección anti-virus, anti-spyware y amenazas. El tráfico al ser inspeccionado por los módulos anti-virus, anti-spyware y de amenazas, puede activar diferentes alarmas o bloqueos dependiendo da cada protección, es decir los tres módulos analizan el tráfico de manera simultáneamente y si detectan una amenaza el módulo toma alguna de las siguientes acciones de manera independiente:

- ***Default:*** para cada evento o grupo de eventos detectado por Palo Alto Networks, se especifica internamente una acción predeterminada. Normalmente, la acción predeterminada es una *alert* o *reset both*.
- ***Allow:*** Permite el tráfico de un evento detectado.
- ***Alert:*** Genera una alerta para el evento detectado y la almacena en un registro de amenazas.
- ***Drop*****:** Bloquea el evento detectado.
- ***Reset Client:*** Para TCP, restablece la conexión del lado del cliente. Para UDP, bloquea la conexión.
- ***Reset Server:*** Para TCP, restablece la conexión del lado del servidor. Para UDP, bloquea la conexión.
- ***Reset Both:*** Para TCP, restablece la conexión tanto en el cliente como en el servidor. Para UDP, bloquea la conexión[42].

8.4.1.4 Modos de configuración del NGFW. A continuación, se realizará una descripción de los modos de configuración del NGFW:

Tap Mode: es un modo de configuración de los Palo Alto que proporciona una forma de acceder a los datos que fluyen a través de una red de manera pasiva. Normalmente para la implementación de modo TAP se requiere de una configuración especial en el switch llamada SPAN o puerto espejo, el cual permite realizar una copia del tráfico de cualquier puerto del switch, de esta manera el puerto SPAN proporciona al NGFW el tráfico duplicado, proporcionando visibilidad del tráfico que atraviesa en la red de manera pasiva.

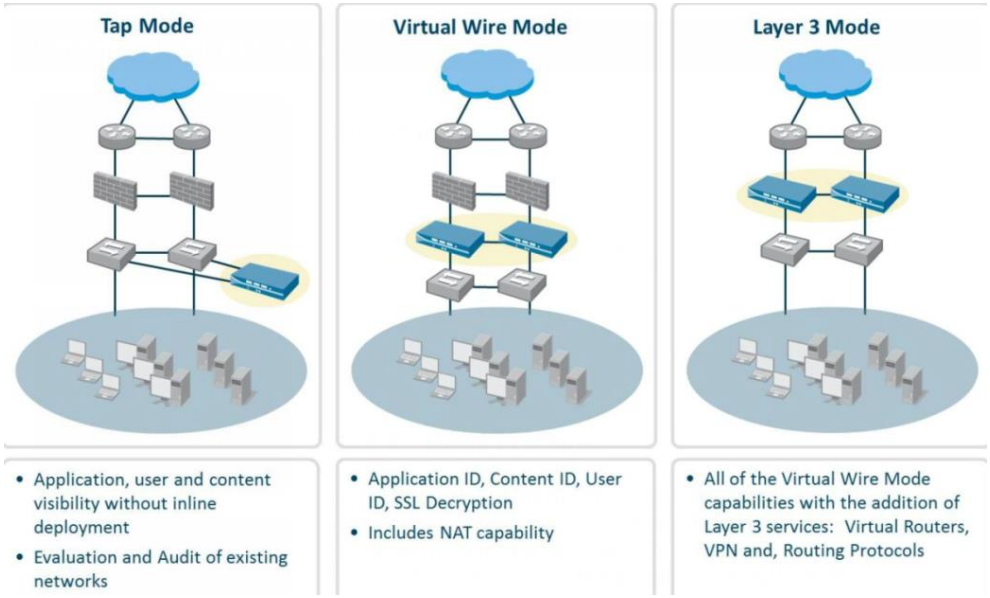
[42] PALO ALTO NETWORK. PAN-OS Administrator's Guide. [En línea], [consultado el 23 de noviembre de 2016]. Disponible en: https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/ framemaker/70/pan-os/pan-os/section_16.pdf. Traducción autor.

Virtual Wire Mode: Este modo el dispositivo visualiza el tráfico que atraviesa por el como cable virtual, es decir funciona en capa 2 del modelo OSI por lo que no requiere enrutamiento, pero a diferencia del *tap mode* el tráfico si atraviesa el dispositivo haciendo parte del flujo de comunicación.

Layer 3 Mode: En una implementación de nivel 3, el NGFW canaliza el tráfico entre varios puertos. Se debe asignar una dirección IP a cada interfaz y se debe definir un enrutador virtual para encaminar el tráfico. Se elige esta opción cuando se requiere enrutamiento.[43]

En la figura 3, se pueden observar los tres modos de configuración explicados anteriormente:

Figura 3. Modos de configuración NGFW



Fuente: PALO ALTO NETWORK. Intrusion Detection System - IDS technology and deployment. [En línea], [consultado el 27 de noviembre de 2016]. Disponible en: https://www.paloaltonetworks.com/documentation/70/pan-os/pan-os/networking/interface-deployments

8.4.2 WAF NetScaler. Citrix NetScaler AppFirewall es una completa Solución de seguridad de aplicaciones web que bloquea ataques conocidos y desconocidos en

[43] PALO ALTO NETWORK. IPS para empresas. [En línea], [consultado el 23 de noviembre de 2016]. Disponible en: https://www.paloaltonetworks.com/documentation/70/pan-os/pan-os/networking/interface-deployments. Traducción autor.

aplicaciones y servicios web. Este dispositivo analiza todo el tráfico de manera bidireccional ya sea de tipo HTTP o cifrado SSL.

Dentro de las reglas de configuración de bloqueo de amenaza a nivel de aplicación que tiene este dispositivo de manera nativa son:

"Deny URL check" Detecta y bloquea conexiones a URLs definidas como amenazas.

"Buffer Overflow check" Detecta los intentos quee provocan desbordamiento de búfer en un servidor web.

"Cookie Consistency check" Detecta modificaciones maliciosas a las cookies establecidas por un sitio web.

"Form Field Consistency check" Detecta modificaciones en la estructura de un formulario web en un sitio web.

"CSRF Form Tagging check" Detecta ataques de falsificación de solicitudes entre sitios.

"Field Formats check" Detecta información inapropiada cargada en formularios web en un sitio web.

"HTML SQL Injection check" Detecta intentos de inyectar código SQL no autorizado.

"HTML Cross-Site Scripting check" Detecta ataques de secuencias de comandos inapropiado de tipo JavaScript o lenguaje similar entre sitios.

Puntos claves de los WAF NetScaler:

- Los firewalls de redes e IPS son útiles para la detección de grandes volúmenes de amenazas en la capa de red y trasporte, pero la mayoría de las tecnologías de seguridad comúnmente implementadas dejan mucho terreno sin cubrir cuando se trata de proteger aplicaciones web.

- Aunque ninguna tecnología de seguridad proporciona protección completa para las aplicaciones web, los WAF son las que más se acercan.

- Combinar NGFW con WAF es una forma eficaz de crear una protección potente y de amplio espectro contra amenazas para todas las propiedades web empresariales importantes.[44]

En la figura 4, se puede observar una comparativa de las tecnologías para proteger las aplicaciones web:

Figura 4. Comparativa de tecnologías para proteger las propiedades web

Comparativa de tecnologías de seguridad para proteger las propiedades web

	Firewall de redes	Sistema de prevención de intrusión	Firewall de próxima generación	Firewall de aplicaciones Web
Funciona en	Capas 3-4	Capas 3-7	Capas 3-7	Capas 3-7+
Arquitectura de despliegue (típica)	Puerta capa 3	Modo transparente	Puerta capa 3	Proxy inverso
Control granular de acceso	Puerto, protocolo, dirección IP	N/C	Puerto, protocolo, dirección IP, usuario, aplicación	Puerto, protocolo, dirección IP
Detección de amenaza/ técnicas de prevención	N/C	Firmas, coincidencia de patrones, y detección de anomalías de protocolo y comportamiento	Firmas, coincidencia de patrones, y detección de anomalías de protocolo y comportamiento	Firmas, detección de anomalías en el protocolo, detección de anomalías en aplicaciones específicas
Cobertura del Protocolo	Cualquiera	Cualquiera	Cualquiera	Centrado en la Web: HTTP(s), XML, SOAP, SPDY
Inspección del tráfico SSL cifrado	N/C	N/C	SÍ	SÍ
Protección DDoS	Capa de red (básica)	Capa de red	Capa de red	Capa de aplicación
Protección de aplicaciones Web	Mínima	Conocido/desconocido vulnerabilidades/ amenazas principalmente para capas de servicios de red y aplicaciones	Conocido/desconocido vulnerabilidades/ amenazas principalmente para capas de servicios de red y aplicaciones	Amplia, incluyendo cobertura completa de la capa de aplicación

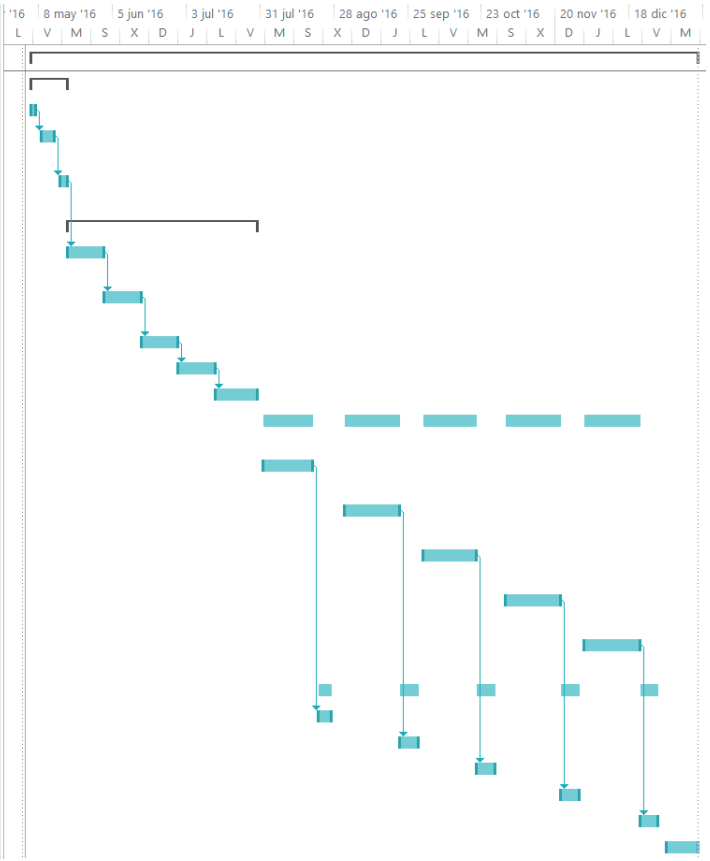
Fuente: CITRIX, Configuring the Application Firewall. [En línea], [consultado el 5 junio de 2016]. Disponible en: http://docs.citrix.com/en-us/netscaler/11/security/application-firewall/configuring-application-firewall.html

44 CITRIX, Configuring the Application Firewall. [En línea], [consultado el 5 junio de 2016]. Disponible en: http://docs.citrix.com/en-us/netscaler/11/security/application-firewall/configuring-application-firewall.html. Traducción autor.

9. CRONOGRAMA

Figura 5. Cronograma

	Modo de	Nombre de tarea	Duración	Comienzo	Fin	Predeceso
1		**CRONOGRAMA**	**181 días**	**jue 5/05/16**	**jue 12/01/17**	
2		**Diagnostico**	**10 días**	**jue 5/05/16**	**mié 18/05/16**	
3		Conocimiento de los activos críticos del MEN	2 días	jue 5/05/16	vie 6/05/16	
4		Estudiar y evaluar las vulnerabilidades internas del MEN.	5 días	lun 9/05/16	vie 13/05/16	3
5		Identificación y análisis de la arquitectura de seguridad perimetral del MEN	3 días	lun 16/05/16	mié 18/05/16	4
6		**Valoración**	**52 días**	**jue 19/05/16**	**vie 29/07/16**	
7		Comparación del dispositivo NGFW Palo alto y Cisco-ASA con la competencia	10 días	jue 19/05/16	mié 1/06/16	5
8		Comparación del dispositivo WAF Net-Scaler con la competencia	10 días	jue 2/06/16	mié 15/06/16	7
9		Estudio características dispositivo NGFW	10 días	jue 16/06/16	mié 29/06/16	8
10		Estudio características dispositivo WAF NetScaler	10 días	jue 30/06/16	mié 13/07/16	9
11		Elaboración de esquema de análisis de IDS y Logs.	12 días	jue 14/07/16	vie 29/07/16	10
12		**Revisión y análisis de IDS y logs dispositivos NGFW (Palo alto y Cisco-ASA) y WAF NetScaler**	**103 días**	**lun 1/08/16**	**mié 21/12/16**	
13		Revisión y análisis de IDS y logs dispositivos NGFW (Palo alto y Cisco-ASA) y WAF NetScaler 1	15 días	lun 1/08/16	vie 19/08/16	
14		Revisión y análisis de IDS y logs dispositivos NGFW (Palo alto y Cisco-ASA) y WAF NetScaler 2	15 días	jue 1/09/16	mié 21/09/16	
15		Revisión y análisis de IDS y logs dispositivos NGFW (Palo alto y Cisco-ASA) y WAF NetScaler 3	15 días	sáb 1/10/16	jue 20/10/16	
16		Revisión y análisis de IDS y logs dispositivos NGFW (Palo alto y Cisco-ASA) y WAF NetScaler 4	15 días	mar 1/11/16	lun 21/11/16	
17		Revisión y análisis de IDS y logs dispositivos NGFW (Palo alto y Cisco-ASA) y WAF NetScaler 5	15 días	jue 1/12/16	mié 21/12/16	
18		**Propuesta de Hardening para NGFW y WAF por RFC**	**104 días**	**lun 22/08/16**	**jue 12/01/17**	
19		Propuesta de Hardening para NGFW y WAF por RFC 1	5 días	lun 22/08/16	vie 26/08/16	13
20		Propuesta de Hardening para NGFW y WAF por RFC 2	5 días	jue 22/09/16	mié 28/09/16	14
21		Propuesta de Hardening para NGFW y WAF por RFC 3	5 días	vie 21/10/16	jue 27/10/16	15
22		Propuesta de Hardening para NGFW y WAF por RFC 4	5 días	mar 22/11/16	lun 28/11/16	16
23		Propuesta de Hardening para NGFW y WAF por RFC 5	5 días	jue 22/12/16	mié 28/12/16	17
24		Generar Informe final	10 días	dom 1/01/17	jue 12/01/17	



Fuente: El autor.

10. ARQUITECTURA

Dentro de los modos de configuración de los NGFW explicados en el numeral 8.4.1.4, se tiene para la sede de DIVEO, configurado en modo *"Layer 3 Mode"* como se observa en la figura 6; y para la sede CAN, se tienen configurados 2 modos con el mismo dispositivo "*Tap Mode"* y "*Layer 3 Mode"*. El *Tap Mode* fue configurado para poder visualizar *malware* e intrusos del MEN de manera pasiva, es decir, funcionando como un IDS permitiendo detectar el tráfico LAN, ya que donde se encuentra ubicado solo puede visualizar la IP NAT del Firewall Cisco ASA como se observa en la figura 7.

De acuerdo a la arquitectura de red ver figura 6 y 7, se observa que no se llevó a cabo una valoración inicial para la adquisición de los NGFW debido a que se evidencio redundancia innecesaria sobre estos dispositivos, en cada una de las sedes de se cuenta con los Palo Alto Networks y adicionalmente para la sede de DIVEO se cuenta Dell Sonicwall y para la sede del CAN se cuenta con Cisco ASA. El motivo de esta redundacia es que inicialmente se contaba con los dispositivos Dell Sonicwall y los Cisco ASA para la sede de DIVEO y CAN respectivamente, pero estos dispositivos no contaban con las bondades de detección de intrusos, *malware,* granularidad y generación de reportes que cuenta los NGFW Palo Alto Networks por este motivo el MEN realizo la adquisición de estos dispositivos, pero sin duda alguna los NGFW Palo Alto pueden realizar de manera simultánea las tareas de firewall, enrutamiento, filtrado de contenido web que realizan los otros dispositivos. Cabe resaltar que los NGFW Dell Sonicwall y Cisco ASA fueron comprados por el MEN y los Palo Alto se encontraban en calidad de arriendo.

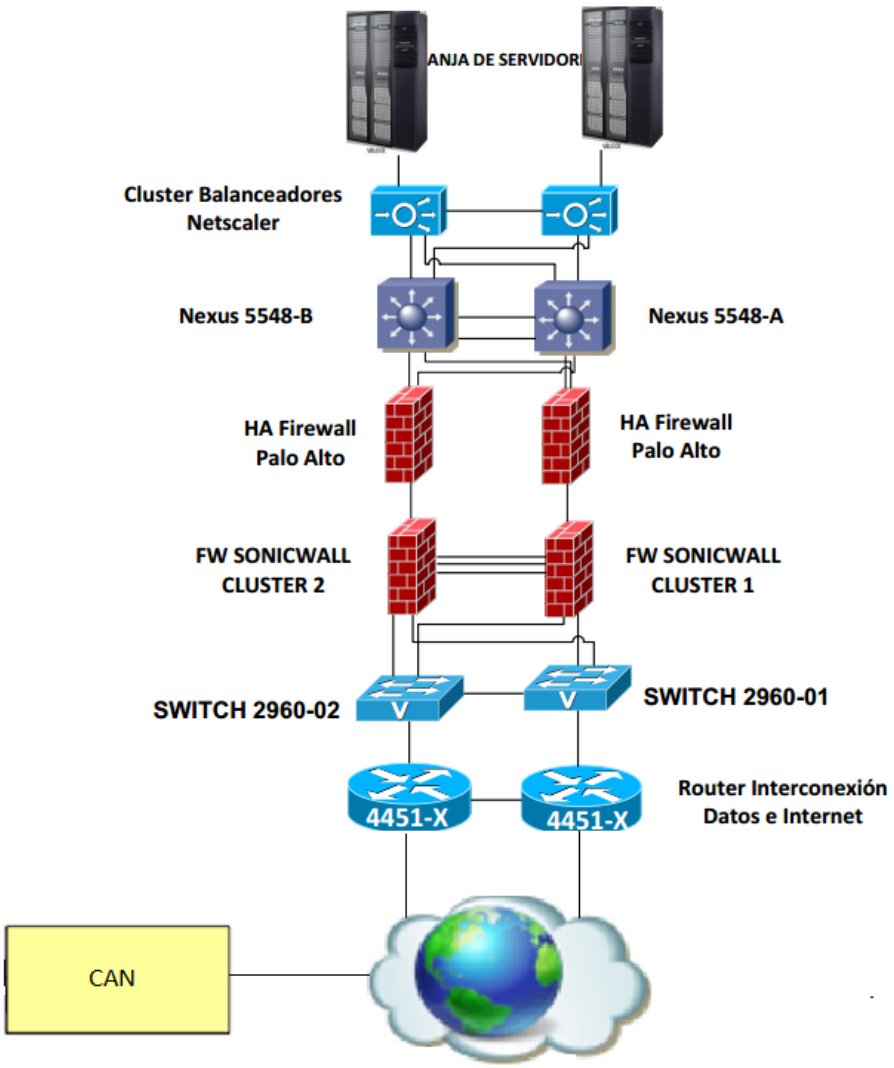
Los dispositivos NetScaler en la sede de DIVEO, adicionalmente a su funcionalidad de WAF se tienen configurados principalmente como balanceadores de carga. En las figuras 7 y 8 se observan las arquitecturas para cada una de las sedes.

10.1 DIVEO

En la sede de DIVEO se encuentran alojados los servidores en ambiente de desarrollo y producción, conectados por los balanceadores NetScaler de Citrix en alta disponibilidad, estos dispositivos también tienen la funcionalidad de WAF, seguidamente se encuentran los switch Nexus en alta disponibilidad, luego están instaladas 2 marcas de NGFW, los Palo Alto Networks y los Dell Sonicwall. El motivo por el cual se tienen 2 marcas NGFW es debido a que los Dell Sonicwall no tienen las bondades de detección y contención de intrusos y/o *malware* que tienen los Palo Alto Networks. Finalmente se encuentran los dispositivos de red que

conectan por medio de una LAN extendida con la sede del CAN y la otra conexión es hacia internet. Lo anteriormente descrito se puede observar en la figura 6:

Figura 6. Diagrama de red –DIVEO



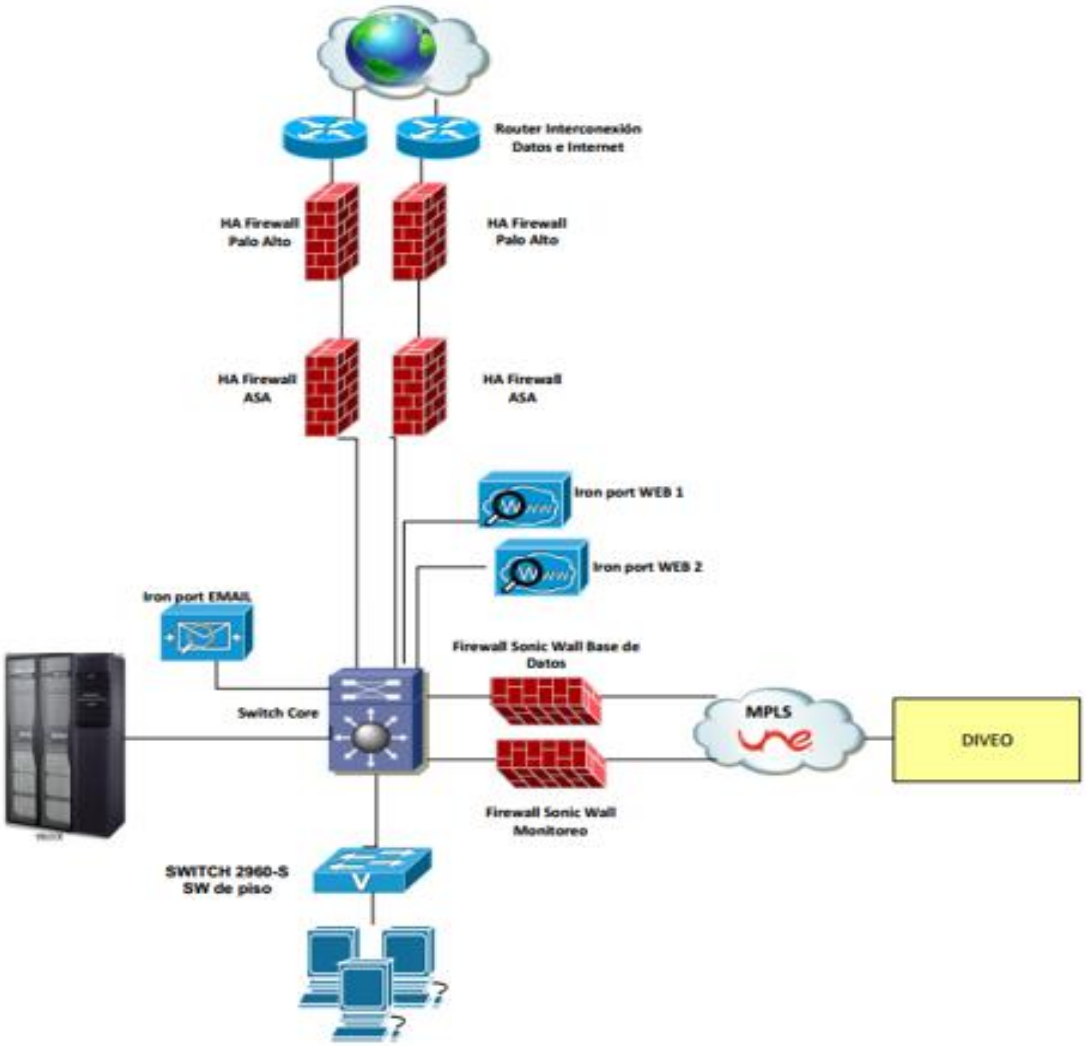
Fuente: El autor.

10.2 CAN

En la sede del CAN, se encuentra el área administrativa donde se ubican los funcionarios y contratistas, adicionalmente están los servidores en ambiente de pruebas conectados a los switches de borde y a su vez conectados al switch Core, el cual interconecta a los dispositivos de seguridad perimetral compuestos por: 2

Iron port Web en alta disponibilidad que tiene como función principal las restricciones de navegación WEB y la contención de *malware* por este medio, un Iron port EMAIL que tiene como funcionalidad de anti-spam, 2 marcas de NGFW una de ellos son los Cisco ASA y la otra son los Palo Alto Networks. El motivo del por qué se cuentan con 2 marcas con la misma funcionalidad, es debido a que los Cisco ASA no cuentan con las bondades de detección y contención de intrusos y/o *malware* que tiene los Palo Alto Networks. Finalmente se encuentran los dispositivos de red que comunican por medio de una la LAN extendida a la sede del CAN y la otra conexión es hacia internet. Lo anteriormente descrito se puede observar en la figura 7:

Figura 7. Diagrama de red – CAN



Fuente: El autor.

11. ANÁLISIS DE RED, DIRECCIONAMIENTO Y PERMISOS DE FIREWALL

En el reconocimiento de red, direccionamiento y permisos de firewall se identificaron los segmentos de red de usuarios y de cada dependencia, al igual que los segmentos de red de los servidores de las zonas de pruebas, desarrollo y producción con los respectivos permisos de firewall, para las sedes de CAN y DIVEO, donde es importante destacar:

Para la sede CAN:

- Los usuarios se encuentran ubicados en la sede de CAN y se encuentran segmentados por VLANs por cada dependencia.
- La conexión inalámbrica WIFI, se encuentra segmentada por 2 SSIDs (Invitados y funcionarios) y la zona se llama WIFI donde el SSID de invitados solo tiene acceso a internet y la de funcionarios tiene acceso a internet y a las aplicaciones misionales del MEN.
- La regla de Firewall de LAN a WAN (Internet) se encuentra permitida por defecto tanto para usuarios como para servidores de los tres ambientes y con pocas restricciones a nivel de filtrado de contenido WEB, lo cual es una mala práctica y debe ser foco de análisis para el dispositivo NGFW de esta sede.
- Los usuarios tienen accesos específicos hacia las zonas DMZ con accesos a los aplicativos misionales con puertos específicos, excepto el segmento de la dependencia de TI que tiene mayores privilegios ya que son los administradores de los servidores que se encuentran en los 3 ambientes.
- La ubicación del NGFW en la arquitectura no permite identificar la IP de cada usuario, debido a que solo ve la IP del NGFW Cisco ASA ya que este dispositivo está realizando NAT a toda la red LAN.

Para la sede DIVEO:

- En esté data center se encuentran ubicados la gran mayoría de servidores del MEN segregados en 2 ambientes de desarrollo y producción, y se llevó la identificación de direccionamiento de acuerdo a la zona.
- Las reglas de firewall por defecto entre zonas tienen como acción *deny* y cuenta con permisos específicos.
- Para los 2 ambientes de servidores se habilita el acceso a internet por demanda, es decir, debe llegar una solicitud formal por parte del cliente donde se indique el servidor, la página a la que quiere acceder y por cuanto tiempo.
- El único ambiente que tiene publicaciones hacia internet es el ambiente de producción, por lo que este direccionamiento será foco de análisis a nivel del NGFW y WAF, debido a que las aplicaciones pueden ser accedidas desde internet considerado como alto riesgo.

Entre las sedes CAN y DIVEO:

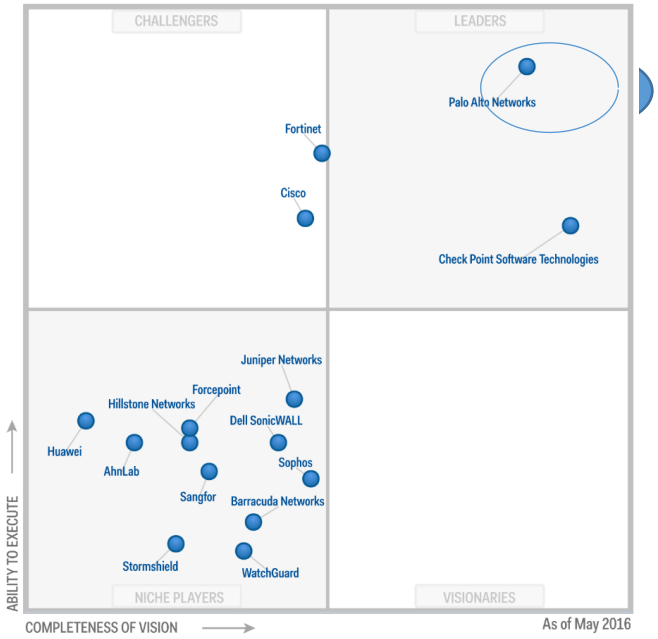
- Lo conexión entre la sede CAN y DIVEO se realiza por medio de un canal dedicado.
- Los usuarios de la sede CAN se conectan hacia las aplicaciones de DIVEO por puertos específicos, cabe destacar que se evidencio mayores accesos a la dependencia de TI, debido a que son los administradores de los servidores, aplicaciones y bases de datos alojados en la sede de DIVEO, este tipo de permisos de la dependencia de TI también serán foco para el análisis de los eventos y alarmas en los NGFW y WAF.

12. VALORACIÓN

La valoración de los dispositivos NGFW y WAF permitirá comparar y evaluar sus fortalezas y debilidades frente a sus competidores, con la finalidad de generar una línea base de su alcance según sus características y en caso de tener limitantes se podrá proporcionar recomendaciones al MEN para la adquisición o renovación de sus productos de seguridad perimetral NGFW y/o WAF.

12.1 COMPARACIÓN NGFW PALO ALTO CON OTROS DISPOSITIVOS

Figura 8. Magic Quadrant for Enterprise Network Firewalls



Fuente: GARTNER, Magic Quadrant for Enterprise Network Firewalls. [En línea], [consultado el 1 junio de 2016]. Disponible en: https://www.gartner.com/doc/reprints?id=1-3805JH8&ct=160525&st=sb

Palo Alto Networks es una compañía de seguridad ubicada en Santa Clara, California, que ha estado vendiendo firewalls **empresariales** desde 2007 y es principalmente conocido por sus innovaciones en el control de aplicaciones e IPS e introducir sistemas basados en la nube y la detección de *malware*. La línea de productos de firewalls incluye 19 modelos, con un rendimiento máximo de 200 Gbps para el PA-7080, lanzado en 2015. El entorno de análisis de *malware* de Palo Alto, como **WildFire** que es un componente de su nube de inteligencia de

amenazas, la cual genero altas tasas de conexión de análisis de amenazas en la nube desde 2015 para los clientes existentes y nuevos.

Palo Alto Networks es evaluado como líder como se observa en la figura 8, debido a su enfoque NGFW y su registro de ofrecer características NGFW por delante de sus competidores respecto a temas de granularidad y profundidad.

12.1.1 Fortalezas. La calidad y facilidad de uso de Palo Alto App-ID e IPS son los dos factores más citados para la selección de este producto sobre otros competidores.

El **Firewall** y el **IPS** están estrechamente integrados, permitiendo detectar e inspeccionar todo el tráfico con sus módulos de anti-spyware, anti-virus y amenazas de manera simultánea o paralela, todas estas soluciones de seguridad en un mismo dispositivo.

En la encuesta a los vendedores, Palo Alto Networks fue el más mencionado como el competidor más fuerte. Los NGFW de Palo Alto continúan apareciendo constantemente en la mayoría de las listas competitivas vistas por Gartner.

El servicio de nube de amenazas avanzadas de WildFire es un complemento popular de los NGFW Palo Alto Networks, proporcionándoles un módulo de análisis de tráfico en busca de detectar nuevas amenazas y *malware;* propiedad de la marca*,* proporcionado una ventaja adicional sobre sus competidores.

12.1.2 Precauciones. Palo Alto Networks se quedó atrás de otros fabricantes líderes en la producción de una versión de firewall virtual para implementaciones como Microsoft Azure.

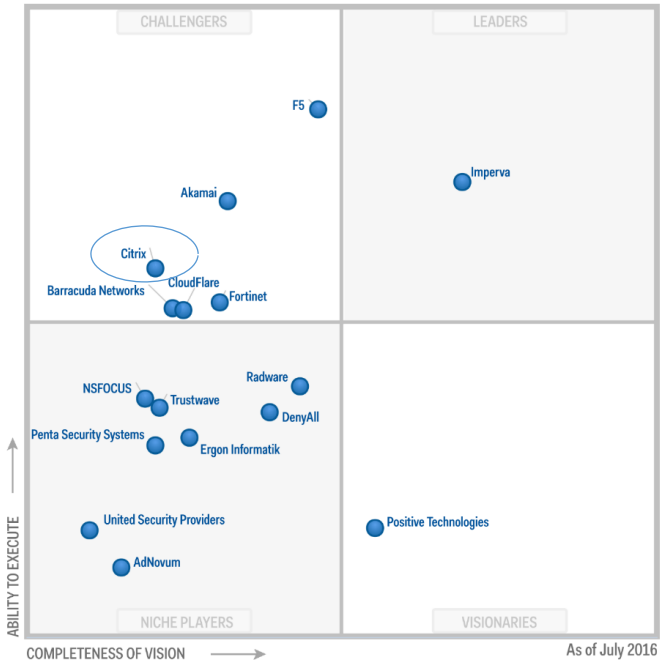
Al igual que otros proveedores con productos líderes, Palo Alto Networks tiene el reto de ganar selecciones en las que los precios se ponderan más que las características de seguridad. Palo Alto tiene uno de los **precios más altos** por gigabit de protección, por arriba de los otros proveedores a nivel de firewall empresarial.

Los clientes de Gartner han señalado la necesidad de un mejor manejo de registros a escala y una disponibilidad de los dispositivos activa/activa. La dirección de Palo Alto es citada como buena superando a los competidores que se encuentran en el cuadrante de Challengers; sin embargo, Gartner aún no ha visto

a Palo Alto posicionarse con éxito hacia los clientes de Firewall debido a que sus productos son muy costosos.[45]

12.2 COMPARACIÓN WAF NETSCALER (CITRIX) CON OTROS DISPOSITIVOS.

Figura 9. Magic Quadrant for Web Application Firewalls



Fuente: GARTNER, Magic Quadrant for Web Application Firewalls. [En línea], [consultado el 5 agosto de 2016]. Disponible en: https://www.gartner.com/doc/reprints?id=1-3BZK2PZ&ct=160720&st=sb

Como se observa en la figura 9 los WAF NetScaler Citrix se encuentran en el nicho de competidores debajo de akamai situándose en una no tan buena posición.

Citrix (CTXS), con sede en Santa Clara, California, y Fort Lauderdale, Florida, es un proveedor global con una amplia cartera de soluciones de virtualización, infraestructura de nube y ADC. Citrix ha ofrecido la funcionalidad de WAF (NetScaler AppFirewall). La línea de productos de hardware de Citrix tiene el

[45] GARTNER, Magic Quadrant for Enterprise Network Firewalls. [En línea], [consultado el 1 junio de 2016]. Disponible en: https://www.gartner.com/doc/reprints?id=1-3805JH8&ct=160525&st=sb. Traducción autor.

nombre de NetScaler MPX, y la línea de dispositivos virtuales tiene el nombre de NetScaler VPX.

Citrix ha lanzado recientemente la reputación IP de NetScaler AppFirewall y ha mejorado el rendimiento del software. En una actualización reciente, el proveedor agregó una sección de seguridad (Security Insight) a su solución centralizada de administración y generación de informes (NetScaler Management and Analytics System).

Citrix es evaluado como *Challenger* porque su solución de WAF (AppFirewall), es una característica adicional en su suite de ADC, y es fácil de habilitar para clientes existentes, **pero rara vez compite en selecciones donde WAF es la principal necesidad.** NetScaler AppFirewall es una buena opción para las organizaciones que buscan una manera fácil de agregar funcionalidades WAF a su inversión existente de Citrix.

12.2.1 Fortalezas. NetScaler SDX incluye soporte que consolida a un gran número de instancias de NetScaler en un solo dispositivo de hardware.

NetScaler AppFirewall proporciona funciones maduras para la seguridad web, incluida la inspección de seguridad para contenido XML y JSON. NetScaler puede agregar compatibilidad transparente para HTTP 2.0 a aplicaciones heredadas. También integra una variedad de características para la optimización del rendimiento de las aplicaciones.

La reciente incorporación de Security Insight al NetScaler agrega un panel de seguridad de alto nivel necesario. El sistema de gestión y análisis de NetScaler incorpora la supervisión del rendimiento de las aplicaciones Web en tiempo real y un panel funcional de certificados SSL.

Los clientes dan altas calificaciones por la facilidad de despliegue de AppFirewall en la plataforma NetScaler y un alto rendimiento, especialmente cuando la mezcla de tráfico incluye un alto porcentaje de tráfico SSL/TLS. NetScaler WAF se puede empaquetar con VPN SSL para acceso remoto a aplicaciones internas.

A diferencia de muchos de sus competidores que proporcionan la reputación de IP como una suscripción pagada, NetScaler lo incluye sin cargo adicional.

12.2.2 Precauciones. NetScaler AppFirewall es un módulo de software del producto ADC y la estrategia del proveedor se ha desplazado para servir a otros mercados distintos a los de seguridad, también se encuentra rezagada detrás de sus competidores al hablar de innovaciones.

Citrix adc frecuencia en las listas de clientes de Gartner, que sus competidores directos por su bajo desempeño a nivel de WAF. La tendencia **en los últimos 12 meses ha sido negativa, con una visibilidad reducida para NetScaler AppFirewall en las listas de favoritos de WAF.**

Gartner no ve el WAF de Citrix desplazando a la competencia basada en sus capacidades de seguridad, sino que la ve como una venta complementaria para las soluciones de ADC.

Citrix no ofrece un servicio de protección DDoS basado en la nube o un WAF basado en la nube. NetScaler sólo puede proporcionar análisis antivirus mediante el reenvío de archivos a terceros.

Los clientes existentes reportan frustración con las funciones de registro y generación de informes. Las funciones de búsqueda están disponibles, pero la función de administración de registro incorporada no ofrece la agregación automática de alertas individuales en eventos correlacionados.[46]

[46] GARTNER, Magic Quadrant for Web Application Firewalls. [En línea], [consultado el 5 agosto de 2016]. Disponible en: https://www.gartner.com/doc/reprints?id=1-3BZK2PZ&ct=160720&st=sb. Traducción autor.

13. DISEÑO METODOLÓGICO

Para el diseño se describirán los componentes que lo involucran y se elaborará un flujo con los responsables del proceso de análisis, aprobación y ejecución del bloqueo de firmas y *malware* a nivel de NGFW y AppFirewall del WAF NetScaler:

A continuación, se describen los componentes que involucran el diseño:

ACTIVOS: Como se describió en el glosario, es todo lo que tiene valor para la organización, ya sea a nivel de hardware o software; para ello se considera importante que el cliente realice una valoración de sus activos y determine el nivel de criticidad según su importancia.

VULNERABILIDADES: como se describió en el glosario, es debilidad de un sistema que permite a un atacante violar la confidencialidad, integridad, disponibilidad, control de acceso y consistencia del sistema o de sus datos y aplicaciones; para ello es importante que se realice un escaneo de vulnerabilidades sobre la infraestructura tecnológica critica, es decir, los servidores.

AMENAZAS: como se describió en el glosario, las amenazas son todo elemento o acción capaz de atentar contra la seguridad de la información; por tal motivo Las amenazas del MEN vistas desde el punto de los dispositivos de seguridad NGFW y WAF pueden ser internas o externas, es decir internas generadas desde la red LAN o DMZs, también pueden ser externas generadas desde la red WAN.

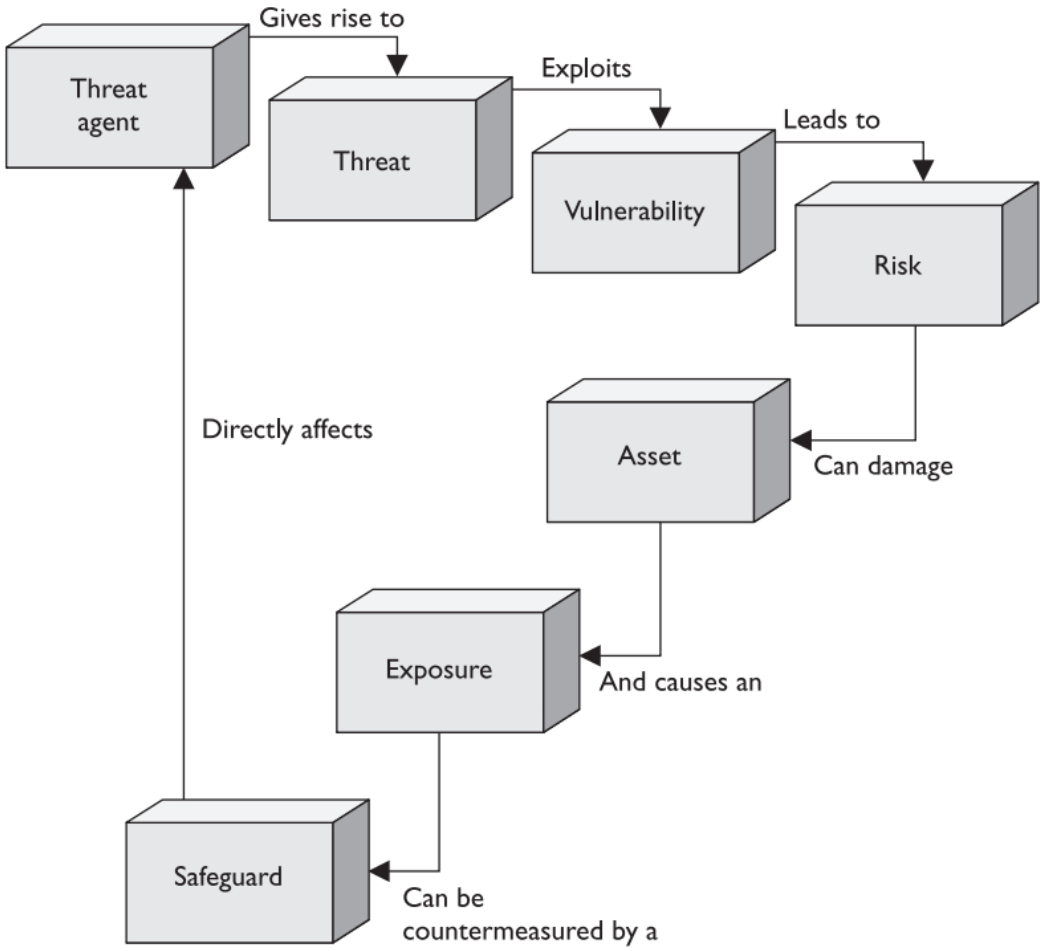
SALVAGUARDAS: De acuerdo al alcance de este proyecto el dispositivo que se va analizar y se va a utilizar como contramedida son los dispositivos NGFW Palo Alto y los WAF NetScaler. En la medida que se realice afinamiento a estos dispositivos va a realizar mayor contención a las amenazas y *malware.*

RIESGO: La probabilidad de que las amenazas internas o externas del MEN se materialice sobre los servidores y/o aplicaciones causando degradación en Organización.

EXPOSICIÓN: Son los puertos y servicios que requieren estar permitidos para poder acceder a los servicios y aplicaciones misionales del MEN; por tal motivo es indispensable realizar un estudio del direccionamiento y permisos de acceso a nivel de firewall perimetral.

En la figura 10, se observa el diseño de conexión de los componentes anteriormente explicados para la mitigación o contención de amenazas.

Figura 10. Esquema de contención de amenazas



Fuente: SHON, Harris. CISSP. 6 ed. United States: American Express, 2013, p.27.

14. FLUJO DE APROBACIÓN FORMAL PARA LAS SOLICITUDES DE AFINAMIENTO SOBRE LOS DISPOSITIVOS

Como uno de los pilares de seguridad es la disponibilidad, se quiere resaltar la importancia de llevar un flujo de aprobación formal, debido a que en el afinamiento de los dispositivos NGFW y WAF existe el riesgo de generar indisponibilidad a nivel de los servicios o funcionalidades de las aplicaciones del MEN, por este motivo se planteó un flujo de aprobación, ver figura 11 en la que cada solicitud formal de afinamiento se realice por medio de correo o por RFC debe ser evaluada y aprobada por el cliente, con el objetivo de minimizar el riesgo ya que es el cliente el que conoce la lógica de negocio. A continuación, se describen las responsabilidades de cada uno actores en el flujograma:

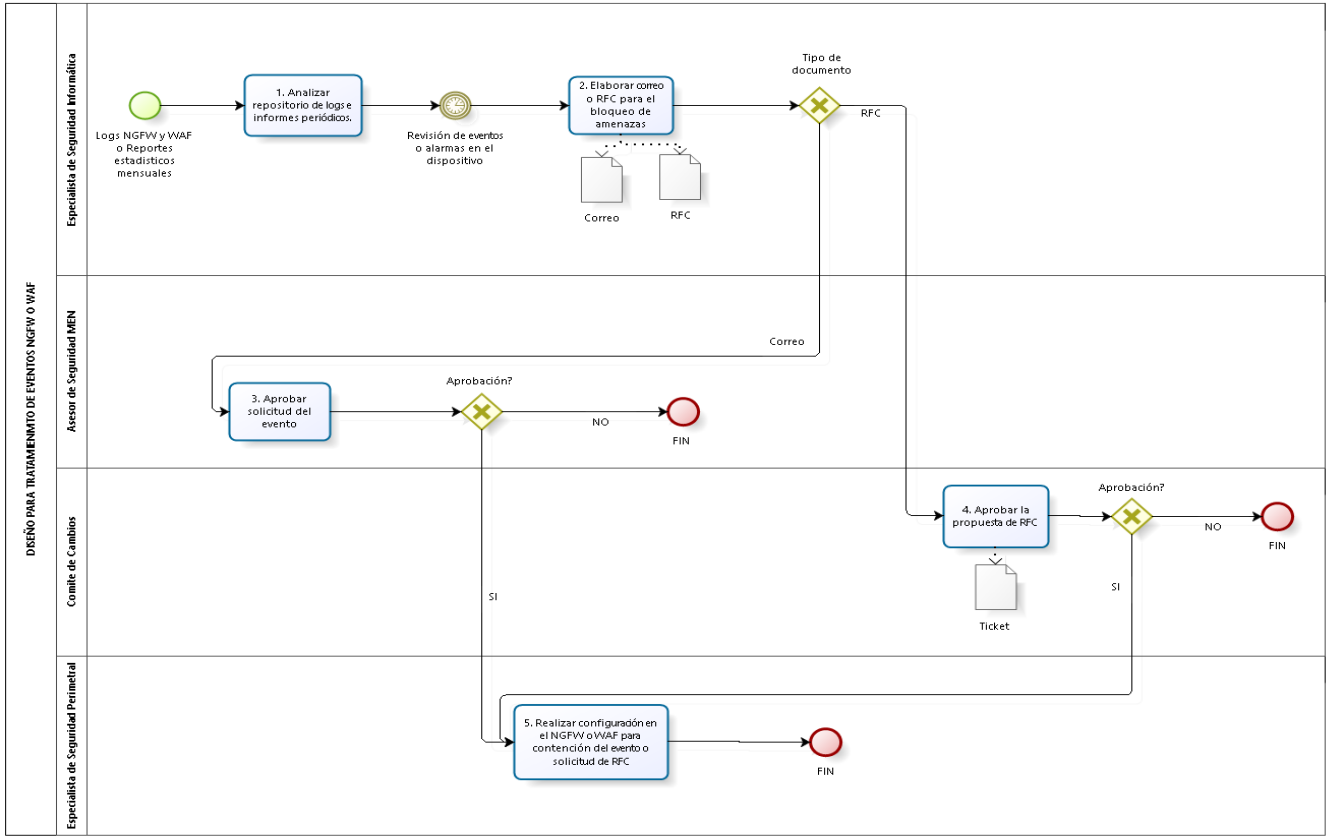
Especialista de Seguridad Informática: Es el analista de los eventos y alarmas de los dispositivos NGFW y WAF (autor del proyecto), que de acuerdo a su inspección solicita realizar afinamiento a los dispositivos NGFW y WAF por medio de correo o RFC para tener aprobación previa del cliente.

Asesor de Seguridad del MEN: Es el autorizador por parte del cliente quien aprueba o deniega la solicitud de afinamiento vía correo enviada por el Especialista de Seguridad Informática.

Comité de Cambios: Es el grupo de personas que dan viabilidad a una solicitud de cambio vía RFC, enviada por Especialista de Seguridad Informática.

Especialista de Seguridad Perimetral: Es el que ejecuta el requerimiento de afinamiento ya que es el administrador de los dispositivos NGFW y WAF del MEN.

Figura 11. Flujograma de eventos NGFW y WAF



Fuente: El autor.

En el cuadro 3, se encuentra la descripción de actividades de los ejecutores definidas en el flujograma de la figura 11.

Cuadro 3. Descripción de actividades

Actividad	Responsable	Registro
1. Analizar repositorio de logs e informes periódicos: El análisis de logs se realiza con los eventos registrados en los dispositivos NGFW y WAF.	• Especialista de Seguridad Informática.	
2. Elaborar correo o RFC para el bloqueo de amenazas: Producto del análisis y detección de eventos en los dispositivos NGFW y WAF se genera un correo si se identifica una amenaza que debe ser bloqueada de manera inmediata o un RFC si es un bloqueo con base a estadísticas de los reportes mensuales.	• Especialista de seguridad informática.	• Correo. • RFC
3. Aprobar solicitud del evento: Si el evento fue generado vía correo especificando las medidas correctivas el aprobador deberá ser el Asesor de Seguridad del MEN.	• Asesor de seguridad informática del MEN.	• Correo.
4. Aprobar la propuesta de RFC: Si el evento fue generado vía RFC especificando las actividades de las medidas correctivas con base a los informes mensuales de seguridad, el aprobador deberá ser el Comité de Cambios del MEN y se generará un ticket para su ejecución.	• Comité de Cambios.	• RFC. • Ticket.
5. Realizar configuración en el NGFW o WAF para contención del evento o solicitud de RFC: Si el Asesor de seguridad o el Comité de Cambios aprueba el correo o el RFC se llevará a cabo las actividades de contención en los dispositivos NGFW y WAF.	• Especialistas de seguridad perimetral.	• Ticket.
Fuente: El autor.		

15. CONOCIMIENTO DE LA CRITICIDAD DE LAS APLICACIONES

El conocimiento de las aplicaciones críticas permitirá priorizar el análisis de los eventos o alarmas generadas sobre los dispositivos NGFW y WAF. En el cuadro 4 se observan las aplicaciones definidas como de alto impacto (categoría 1) y en el cuadro 5 las aplicaciones definidas como de medio impacto (categoría 2).

15.1 APLICACIONES CATEGORÍA 1

El grupo de las aplicaciones categoría 1 cumplen con las siguientes características:

- Aplicaciones de gran impacto o misión crítica para el MEN y el Sector Educativo Colombiano.
- En este grupo de aplicaciones se encuentran las que registran mayor transaccionalidad especialmente desde las Secretarías de Educación Nacional.

Cuadro 4. Aplicaciones Categoría 1

Aplicaciones categoría 1		
Correo Electrónico	PRAE - Proyectos Ambientales Escolares	SINEB
CNA	RRHH - Secretarías	SIPI
Convalidaciones Educación Superior	SACEN	SNIES
Delegados y Representantes	SGCF - Sistema de Información de gestión y Control Financiero Secretarias de Educación	SPADIES
Evaluación De Competencias Para Ascenso Y Reubicación Salarial	SICIED WEB	VUMEN
EVI	SIET	Asistencia Técnica
Gratuidad. Este es el mismo SIFSE	SIGCE	SAC - Secretarías
OLE	SIMAT	SIEE
Perfiles Territoriales	SIMPADE	SACES
Fuente: MEN.		

15.2 APLICACIONES CATEGORÍA 2

El grupo de las aplicaciones categoría 1 cumplen con las siguientes características:

- Aplicaciones de impacto medio para el MEN y para el Sector Educativo.
- En este grupo de aplicaciones se encuentran sistemas con poca cantidad de registros, y con una baja transaccionalidad para las bases de datos y para el canal de Internet.

Cuadro 5. Aplicaciones Categoría 2

Aplicaciones categoría 2		
Directorio Intranet (Integración con LDAP)	Catálogo de Textos y Libros Escolares	SACEN - Sistema de Aseguramiento de la Calidad de las Escuelas Normales
SIGA - Sistema para la Interventoría y Gestión de Alianzas	CONPES - Consolidación de Información Primera Infancia	SIMEN - Sistema de Información de Buenas Prácticas
Reporte de Inventario a Conexión Total	Consulta de Títulos de Educación Superior	Sistema de Apoyo de Transformación de la Calidad Educativa
Buscando Posgrado	Desprendibles de Pago	Sistema de Atención al Ciudadano - SAC - Modernización
Buscando Colegio	LMCS - Sistema Administración de Contenidos	Sistema Unificador de Primera Infancia
Buscando Pregrado	Nivelación Salarial - Versionador	SQI - Seguimiento a Quejas e Investigaciones
Fuente: MEN.		

16. ANÁLISIS DE VULNERABILIDADES

El escaneo de vulnerabilidades se realizó entre el 15 y el 28 mayo de 2016 en los servidores de la red interna del MEN tanto para los servidores del CAN como de DIVEO y la herramienta utilizada fue el software Nessus Professional. Antes de realizar el escaneo, a la dirección IP del equipo en el que se encontraba instalado el Nessus se habilitaron permisos de firewall para poder acceder a los segmentos de red a evaluar, tanto en CAN, como en DIVEO, ya que por defecto en cualquier punto de red del CAN no es posible acceder directamente a todos los servidores.

El análisis se realizó sin usuario autenticado y sin vectores de evaluación de denegación de servicio. La calificación de las vulnerabilidades se realiza a través de CVE *(Common Vulnerabilities and Exposures).* En los casos cuando la vulnerabilidad no encuentra un CVE, pero ha sido confirmada por el fabricante, se califica por defecto con severidad *high*.

En el anexo A, se puede observar a nivel de informe ejecutivo el resultado del escaneo de vulnerabilidades, donde en las gráficas 16 y 17, se pueden visualizar que fueron identificadas aproximadamente en los mismos porcentajes en la clasificación por severidades para las dos sedes CAN y DIVEO, alcanzando un promedio de 75% con severidad *medium*, 14% *informative*, 8% *high* y 3% *critical*, es importante destacar que las vulnerabilidades detectadas por la herramienta Nessus son a nivel de infraestructura (Sistemas Operativos, servidores y aplicaciones), el cual fueron un insumo para enfocar el análisis de logs del NGFW y WAF. Para fines de este proyecto el resultado del escaneo se clasificará y categorizará las vulnerabilidades de tipo *critical* y *high* que son lo que se consideran de alto impacto.

En las gráficas 16 y 17 del anexo A, se puede apreciar que varias de las vulnerabilidades se encuentran asociadas a la falta de actualizaciones de software de capa media, software sin soporte, actualizaciones de sistema operativo, por lo tanto para el análisis de eventos y alarmas de los dispositivos de NGFW y WAF, se tendrán presente los que en sus registros tengan firmas relacionadas con las aplicaciones *middleware* como Tomcat, Jboss, Oracle, PHP y Apache entre las zonas de internet hacia la DMZ de producción, debido a que estas vulnerabilidades pueden ser explotadas desde internet, para las vulnerabilidades asociadas a sistemas operativos sin soporte se debe tener presente los registros de eventos y alarman entre las zonas de LAN hacia las DMZs en especial el segmento de red donde se encuentra el área de TI, debido a que esta área tiene privilegios y permisos hacia la red de servidores para su administración y pruebas.

En las gráficas 18 a la 25, se generó una clasificación de vulnerabilidades por área a nivel de bases de datos, infraestructura y aplicaciones con sus respectivas

vulnerabilidades, en las que se tendrán las siguientes consideraciones en la revisión de eventos, alarmas e informes de los NGFW y WAF:
Para bases de datos:

- Envenenamiento de Oracle listener - CVE-2012-1675.
- Oracle sin soporte.

Para infraestructura:

- Sistemas operativos sin soporte.

Para aplicaciones:

- Apache con versiones obsoletas o sin soporte.
- PHP con versiones obsoletas o sin soporte.
- Weblogic permite ejecución de comandos de manera remota.
- Jboss permite ejecución de comandos de manera remota.

17. ANÁLISIS DE TAP NGFW SEDE CAN

De acuerdo a la arquitectura de la sede del CAN ver numeral 10.2, los NGFW Palo Alto se encuentran ubicados entre los routers de borde y los Cisco ASA, por lo que al analizar los eventos y alarmas en los Palo Alto solo se observa la IP NAT de los Cisco ASA sin poder identificar las IPs de los endpoints o servidores, para solucionar este inconveniente se utilizaron unas interfaces libres de los Palo Alto para ser configuradas en modo TAP, este modo fue explicado en el numeral 8.4.1.4, cabe indicar que este modo solo permite la identificación de intrusos o *malware* de forma pasiva, es decir, funcionando como un IDS.

Con base al anexo B, se pudo observar que se llevó a cabo la identificación varios eventos maliciosos en la sede CAN apoyado en la configuración de modo TAP y posteriormente se reportaron vía correo hacia el asesor de seguridad del MEN para su revisión y toma de medidas preventivas y/o correctivas, de acuerdo al flujograma de escalamiento establecido, ver figura 11, en estos correos fueron reportados todos los eventos detectados en los NGFW del CAN sobre los *endpoints* que tenían alto indicio de estar infectados por *malware*, con el objetivo que se tomaran las medidas correctivas y/o preventivas, la cual consistía en aislar la máquina, validar el estado del antivirus local y realizar un escaneo.

Se puede concluir que la implementación de modo TAP genero gran valor para la identificación de los *endpoints* infectados al interior del MEN, el cual se evidencio que algunos *endpoints* no contaban con antivirus instalado o se encontraba desactualizado como se observa en el anexo B. El *malware* identificado corresponde la gran mayoría a spyware y como se describió en el numeral 8.4.1.2 donde explica el comportamiento de este *malware*, el cual consiste en infectar a la víctima ubicada en la red LAN y posteriormente envía tráfico saliente al equipo atacante ubicado en la red WAN (internet), cabe destacar, que si no se tuviera configurado el modo TAP no sería posible identificar los equipos infectados, debido a que solo podría visualizar la IP NAT de los Cisco ASA.

18. RESULTADO FINAL DEL ANÁLISIS DE LOS NGFW Y WAF

En el anexo C se encuentran consolidadas las gráficas estadísticas a partir del mes de mayo hasta el mes de diciembre de 2016, período al que se hace referencia en el cronograma que se encuentra en el numeral 9; para la generación de las gráficas fue necesario ponderar manualmente los logs del módulo de amenazas, anti-virus y anti-spyware de los dispositivos NGFW para las sedes DIVEO y CAN, las gráficas generadas son:

- Top de amenazas por firma.
- Top de servidores con más eventos de amenazas.
- Acciones por severidad *critical* y *high*.

Para el módulo de anti-virus y anti-spyware solo se registraron eventos en la sede CAN, generando el top de las siguientes categorías:

- Anti-Virus.
- Anti-Spyware.
- Eventos Wildfire

Las gráficas estadísticas ponderadas de los logs del dispositivo WAF, para la sede de DIVEO son:

- Top amenazas por firmas.
- Top sitios web con más eventos.
- Top bloqueo por firmas.

Es importante indicar que no se contó con una herramienta SIEM *(Security Information and Event Management)*, la cual permite correlacionar eventos de diferentes dispositivos generando reportes y gráficas estadísticas de los mismos, sino que las gráficas generadas para cada uno de los dispositivos NGFW y WAF, fueron tomadas directamente de los logs de estos dispositivos y posteriormente procesadas manualmente.

Los dispositivos NGFW y WAF se encontraban instalados antes de la realización del presente documento por lo que contaban con una configuración inicial y luego del proceso de valoración, análisis e investigación que se realizó, se procedió con el afinamiento de los dispositivos de manera controlada de acuerdo a los eventos registrados y analizados en cada sede.

El objetivo del análisis de las gráficas generadas mensualmente, ver anexo C, era estudiar las firmas que se encontraban permitidas en el módulo de amenazas, anti-virus y anti-spyware, para que a partir de este análisis se determinara si la

firma(s) podrían corresponder a una amenaza o un falso positivo, pero para llegar a esta conclusión final era necesario la participación y aprobación del MEN y del grupo de auditoria, el cual se llevaba a cabo por medio de un comité de cambios en donde se sustentaba el RFC dando a conocer el resultado del análisis, finalmente si las partes en común acuerdo determinaban que correspondía a una amenaza se aprobaba el bloqueo de la firma(s) o de lo contrario la firma era considerada falso positivo y no se realizaba ninguna acción.

Para el bloqueo de una categoría ya sea de tipo críticas, altas, medias, bajas o informativas era necesario que la categoría a bloquear tuviera previamente varias firmas consideradas como amenazas y que el bloqueo de estas no hubiera generado ninguna indisponibilidad en las aplicaciones del MEN, de igual manera esta solicitud de bloqueo de una categoría se llevaba a cabo de manera formal y sustentada en un comité de cambios, pero si por lo contrario la categoría tenía firmas bloqueadas y otras permitidas por que eran consideradas como falsos positivos la categoría no podría ser bloqueada y se tendría que continuar analizando firmas puntuales, la acción de bloqueo de firmas puntuales sobre una categoría se le denomino *custom.*
En el cuadro 6 se observa la configuración inicial antes del mes de mayo y luego del proceso de afinamiento hasta el mes de diciembre para los dispositivos NGFW de CAN y DIVEO:

Cuadro 6. Configuración Mayo vs. Diciembre para los NGFW de DIVEO y CAN

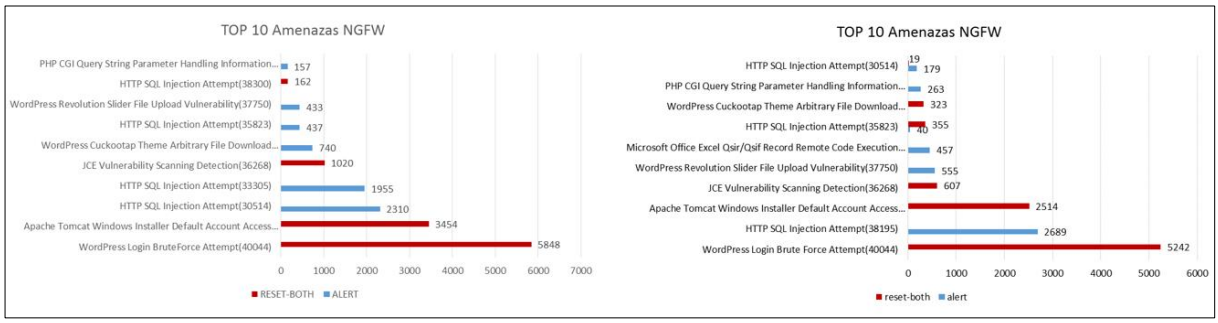
		CAN - mayo			CAN - diciembre			DIVEO - mayo			DIVEO - diciembre		
Modules	Categories	Block	Alert	Custom	Block	Alert	Custom	Block	Alert	Custom	Block	Alert	Custom
Threats	Criticas	X			X			X			X		
	Altas	X			X			X			X		
	Medias		X				X		X				X
	Bajas		X				X		X				X
	Info		X			X			X			X	
Spyware	Criticas	X			X				X		X		
	Altas		X		X				X		X		
	Medias		X		X				X		X		
	Bajas		X		X				X		X		
	Info		X			X			X			X	
Anti-Virus	http	X			X				X		X		
	smtp	X			X				X		X		
	imap	X			X				X		X		
	pop3	X			X				X		X		
	ftp	X			X				X		X		
	smb	X			X				X		X		
WildFire	Malware		X		X				X		X		
	Greyware		X			X			X			X	
	Bening		X			X			X			X	

Fuente: Configuración de los dispositivos NGFW de DIVEO y CAN.

18.1TOP DE AMENAZAS POR FIRMA – DIVEO Y CAN

Para la gráfica 1, se observa que en el mes de mayo en el top 10 de amenazas del NGFW de DIVEO se encuentran 4 bloqueadas, mientras que para el mes de diciembre se observan 6 firmas bloqueadas, es importante destacar que dentro de las 6 firmas bloqueadas del mes de diciembre 2 de ellas "*HTTP SQL Injection Attemp* (30514)" y "*HTTP SQL Injection Attemp* (35823)" cuentan con 2 barras de manera simultánea; una de color rojo, que traduce tráfico bloqueado y la otra de color azul, que traduce tráfico permitido, el motivo es debido a que el proceso de solicitud de bloqueo se generó en el mes de diciembre, es decir que en el top 10 de amenazas del mes de noviembre se encontraban permitidas (ver gráfica 86), esto explica la dinámica del modelo de afinamiento, donde mes a mes se analizaban las firmas que se encuentran permitidas, para evaluar si corresponden a una amenaza o a un falso positivo. De considerarse una amenaza se procedía a solicitar su bloqueo por medio del CAB. Las firmas que se encuentran permitidas en la categoría top 10 de amenazas y se repiten mes a mes, es debido a que luego de un análisis a profundidad fueron catalogadas como falsos positivos.

Gráfica 1. Top 10 amenazas mayo vs diciembre – DIVEO



Fuente: Logs NGFW DIVEO mayo y diciembre de 2016.

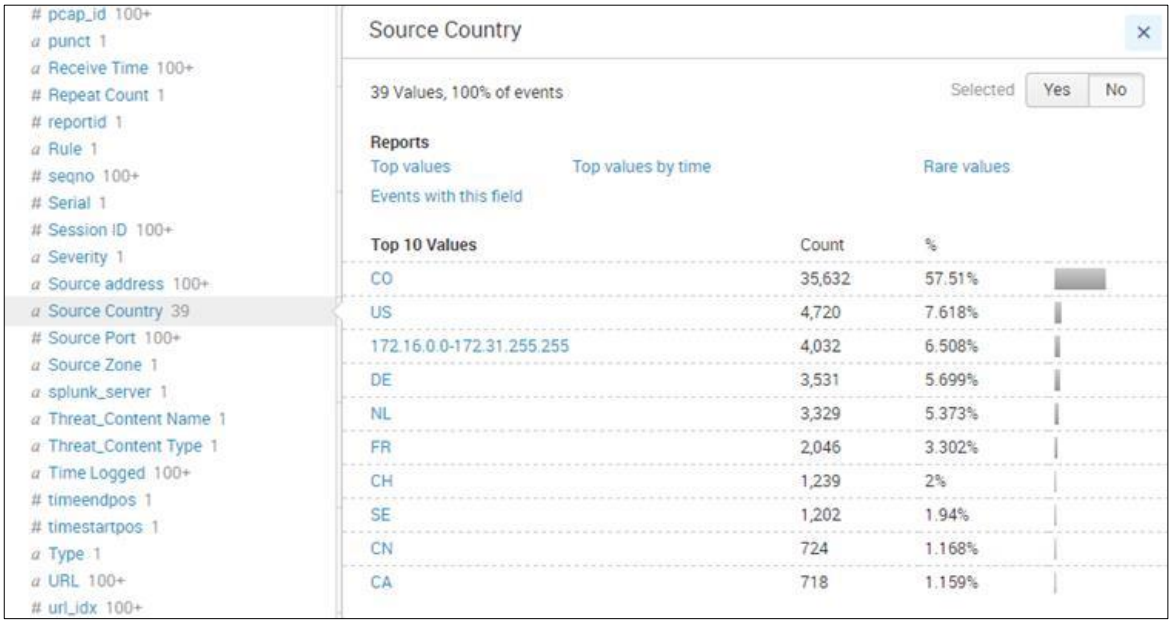
Las 2 firmas con ID 30514 y 35823 corresponden a SQL *Injection* el cual, es una técnica para explotar una vulnerabilidad de seguridad que ocurre en la capa de base de datos por medio de una aplicación, adicionalmente dentro del Top 10 de OWASP el ataque de *SQL Injection* se encuentra en la posición número 1.

Con el objetivo de dar a conocer una muestra del análisis para solicitar el bloqueo de cada una de las firmas "*HTTP SQL Injection Attemp* (30514)" y "*HTTP SQL Injection Attemp* (35823)" en el mes de diciembre de 2016 para la sede de DIVEO, se describirá a continuación el proceso de análisis para cada una de las firmas.

- FIRMA: *HTTP SQL Injection Attempt* (30514):

En la gráfica 2 se observa el país origen que activó esta firma, la cantidad de tráfico generado y su porcentaje; el cual permite indagar si es perteneciente a un intento de ataque informático basándose en la premisa que la gran mayoría de acceso hacia las páginas del MEN debe ser originado desde el país colombiano.

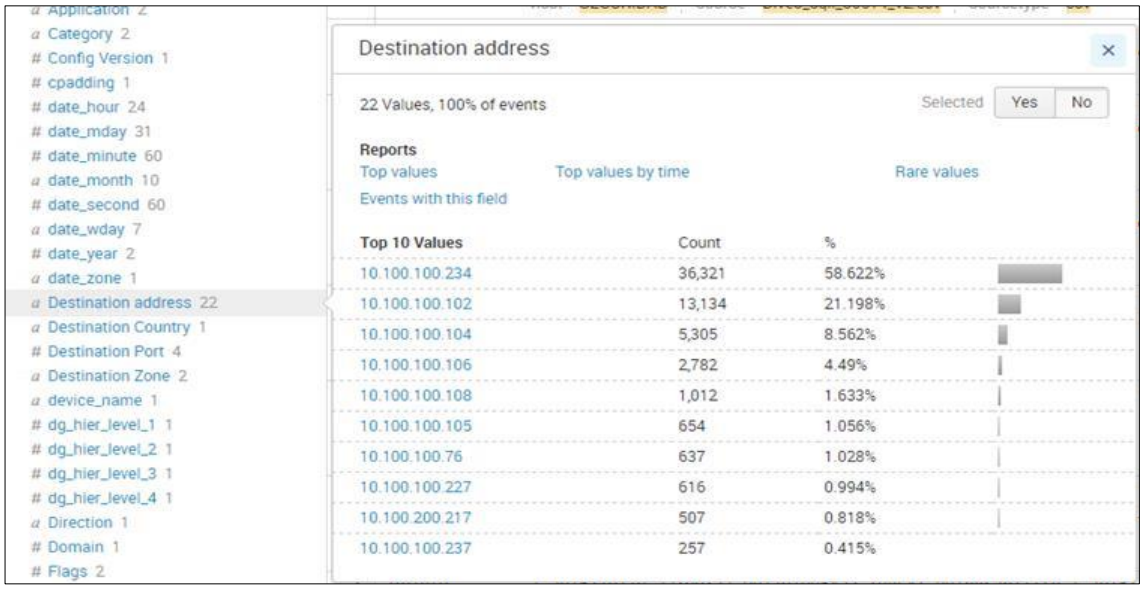
Gráfica 2. Países de origen que activaron la firma *HTTP SQL Injection Attempt* (30514)



Fuente: Logs NGFW DIVEO diciembre de 2016.

En la gráfica 3, se observa el direccionamiento destino relacionado con la firma *HTTP SQL Injection Attempt* (30514), donde se detalla la dirección IP, cantidad de tráfico y su porcentaje; estos datos permiten detectar cual es el servidor que está recibiendo este tipo de tráfico y posteriormente validar a nivel de host, los logs a nivel de aplicación, eventos del antivirus local, script defacement, entre otros. Como resultado se determinará si el servidor fue comprometido y si está asociado a la firma detectada.

Gráfica 3. Direccionamiento destino a la que va dirigido el tráfico asociado firma *HTTP SQL Injection Attempt* (30514)



Fuente: Logs NGFW DIVEO diciembre de 2016.

En el cuadro 7 se relacionan las URLs asociadas a las IPs detectadas en la gráfica 3, el cual es un insumo importante para la sustentación del RFC, donde el cliente conociendo la lógica de la entidad y la criticidad de la aplicación (ver numeral 15), aprueba o deniega la solicitud de bloqueo de esta firma.

Cuadro 7. Relación de la identificación de las páginas con el direccionamiento de la firma *HTTP SQL Injection Attempt* (30514)

HTTP SQL Injection Attempt (30514)		
Porcentaje	IP	URL
58,6%	10.100.100.234	http://rrhh.gestionsecretariasdeeducacion.gov.co:2383
21,2%	10.100.100.102	17 Secretarías
8,6%	10.100.100.104	http://www.sedmagdalena.gov.co
	10.100.100.104	http://www.semduitama.gov.co
4,5%	10.100.100.106	http://www.sedarauca.gov.co
	10.100.100.106	http://www.sedputumayo.gov.co
	10.100.100.106	http://www.sedmeta.gov.co
1,6%	10.100.100.108	http://www.sedbolivar.gov.co/
	10.100.100.108	http://www.sedsucre.gov.co
	10.100.100.108	http://www.semcucuta.gov.co
	10.100.100.108	http://www.semsincelejo.gov.co

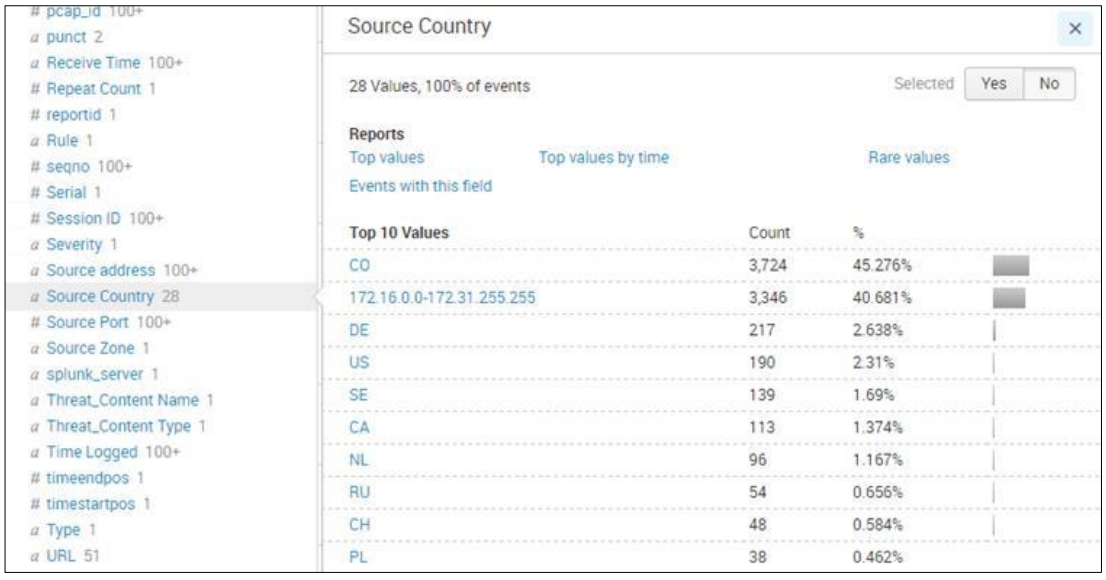
Fuente: Logs NGFW DIVEO diciembre de 2016 y CMDB.

Como conclusión, se observó en la gráfica 2, que el país o red origen que activó la firma *HTTP SQL Injection Attempt* (30514) es en primer lugar Colombia con el 58.6%, en segundo lugar Estados Unidos con el 21.2% y en tercer lugar el segmento de red 172.16.X.X correspondiente a red interna Colombia Compra Eficiente con el 8,5%, por lo que se concluye que gran parte del tráfico generado hace parte de consultas del interior del país, por lo que hay altas probabilidades que sea un falso positivo, de igual manera se sugiere el bloqueo de esta firma con el objetivo de preservar la integridad, confidencialidad y disponibilidad de los aplicativos que contienen las URLs descritos en el cuadro 7, adicionalmente se sugiere que si luego de activar el bloqueo de las firmas llegase a presentarse un bloqueo a nivel de funcionalidad, se cree una exclusión específica indicando la IP origen y destino, pero sin desactivar el bloqueo de la firma.

- FIRMA: *HTTP SQL Injection Attempt* (35823).

En la gráfica 4 se puede visualizar el país origen que activó esta firma, la cantidad de tráfico generado y su porcentaje, el cual permite indagar si es perteneciente a un intento de ataque informático, basándose en la premisa que la gran mayoría de acceso hacia las páginas del MEN debe ser originado desde el país colombiano.

Gráfica 4. Países de origen que activaron la firma *HTTP SQL Injection Attempt* (35823)



Fuente: Logs NGFW DIVEO diciembre de 2016.

En la gráfica 5, se puede visualizar el direccionamiento destino relacionado con la firma *HTTP SQL Injection Attempt* (35823), donde se detalla la dirección IP,

cantidad de tráfico y su porcentaje, estos datos permiten detectar cual es el servidor que está recibiendo este tipo de tráfico y posteriormente validar en el servidor de manera local, los logs a nivel de aplicación, eventos del antivirus local, *script defacement*, entre otros, y como resultado se determinará si el servidor fue comprometido y si está asociado a la firma detectada.

Gráfica 5. Direccionamiento destino asociado a la firma *HTTP SQL Injection Attempt* (35823)

Fuente: Logs NGFW DIVEO diciembre de 2016.

En el cuadro 8 se relacionan las URLs asociadas a las IPs detectadas en la gráfica 5, el cual es un insumo importante para la sustentación del RFC, donde el cliente conociendo la lógica de la entidad y la criticidad de la aplicación (ver numeral 15), aprueba o deniega la solicitud de bloqueo de esta firma.

Cuadro 8. Identificación de las páginas con el direccionamiento a las que va dirigido el tráfico de la firma *HTTP SQL Injection Attempt* (35823)

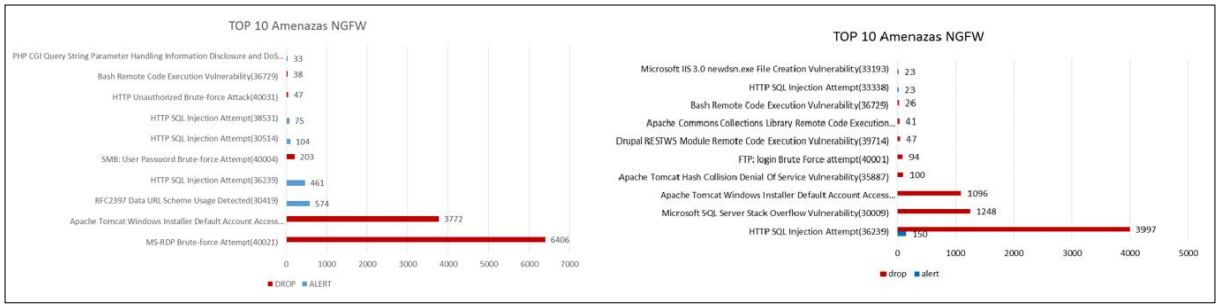
HTTP SQL Injection Attempt (35823)		
Porcentaje	**IP**	**URL**
40,4%	10.100.100.234	http://rrhh.gestionsecretariasdeeducacion.gov.co:2383
39,2%	10.100.100.104	http://www.sedmagdalena.gov.co
	10.100.100.104	http://www.semduitama.gov.co
4,9%	10.100.100.102	17 Secretarías

Fuente: Logs NGFW DIVEO diciembre de 2016 y CMDB.

Como conclusión, se observa en la gráfica 4, que el país o red origen que activó la firma *HTTP SQL Injection Attempt* (30514) es en primer lugar Colombia con 45,2%, en segundo lugar la red 172.16.X.X correspondiente a Colombia Compra Eficiente con el 40.6% y en tercer lugar Alemania con el 2.6%, por lo que se concluye que gran parte del tráfico generado hace parte de consultas del interior del país, por lo que hay altas probabilidades que sea un falso positivo, de igual manera se sugiere el bloqueo de esta firma con el objetivo de preservar la integridad, confidencialidad y disponibilidad de los aplicativos que contienen las URLs descritos en el cuadro 8, adicionalmente se sugiere que si luego de activar el bloqueo de las firmas llegase a presentarse un bloqueo a nivel de funcionalidad se cree una exclusión específica indicando la IP origen y destino, pero sin desactivar el bloqueo de la firma

En la gráfica 6, se observa que en el mes de mayo del top 10 de amenazas del NGFW de CAN se encuentran 5 bloqueadas, mientras que para el mes de diciembre se encuentran 8 firmas bloqueadas y 1 de ellas denominada "*HTTP SQL Injection Attemp* (36239)" cuenta con 2 barras de manera simultánea; una de color rojo, que traduce tráfico bloqueado y la otra azul que traduce tráfico permitido, para esta firma, el proceso de solicitud de bloqueo se generó en el mes de diciembre, el motivo por el cual específicamente esta firma fue bloqueada en este mes, es debido a que en el top 10 de amenazas para el de mes de noviembre se encontraba permitida (ver gráfica 93), esto explica la dinámica del modelo de afinamiento, donde mes a mes se analizaban las gráficas estadísticas especialmente las firmas que se encuentran permitidas, para evaluar si correspondían a una amenaza o a un falso positivo. De considerarse una amenaza, su aprobación de bloqueo ser realizaba por medio del CAB. Las firmas que se encuentran permitidas en la categoría top 10 de amenazas y se repiten mes a mes, es debido a que luego de un análisis a profundidad fueron catalogadas como falso positivo.

Gráfica 6. Top 10 amenazas mayo vs diciembre – CAN



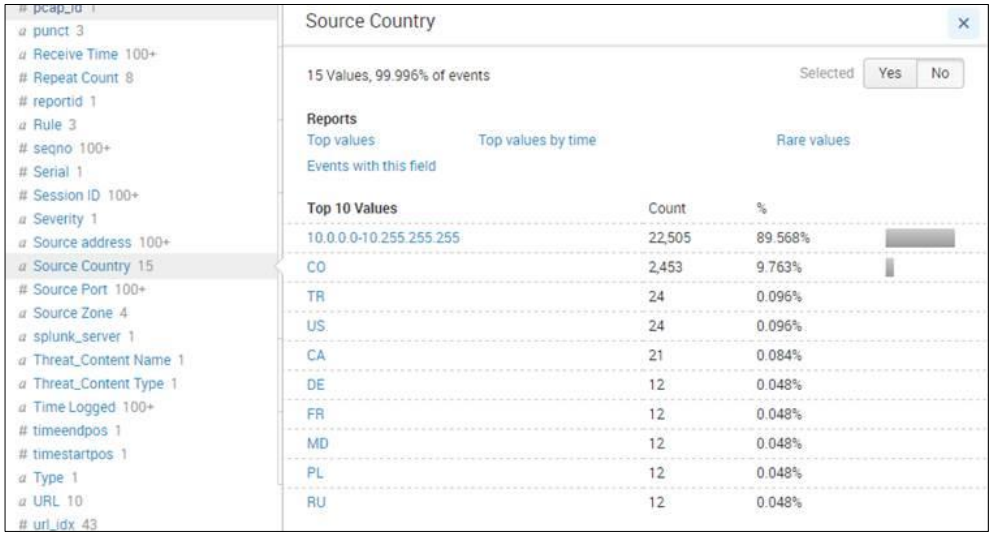
Fuente: Logs NGFW CAN Mayo y diciembre de 2016.

Con el objetivo de dar a conocer una muestra del análisis para solicitar el bloqueo para la firma "*HTTP SQL Injection Attemp* (36239)" del mes de diciembre de 2016 para la sede de CAN, se describirá a continuación el proceso de análisis para esta firma.

- FIRMA: *HTTP SQL Injection Attempt* (36239)

En la gráfica 7 se observa el país origen que activó esta firma, la cantidad de tráfico generado y su porcentaje, el cual permite indagar si es perteneciente a un intento de ataque informático basándose en la premisa que la gran mayoría de acceso hacia las páginas del MEN debe ser originado desde el país colombiano.

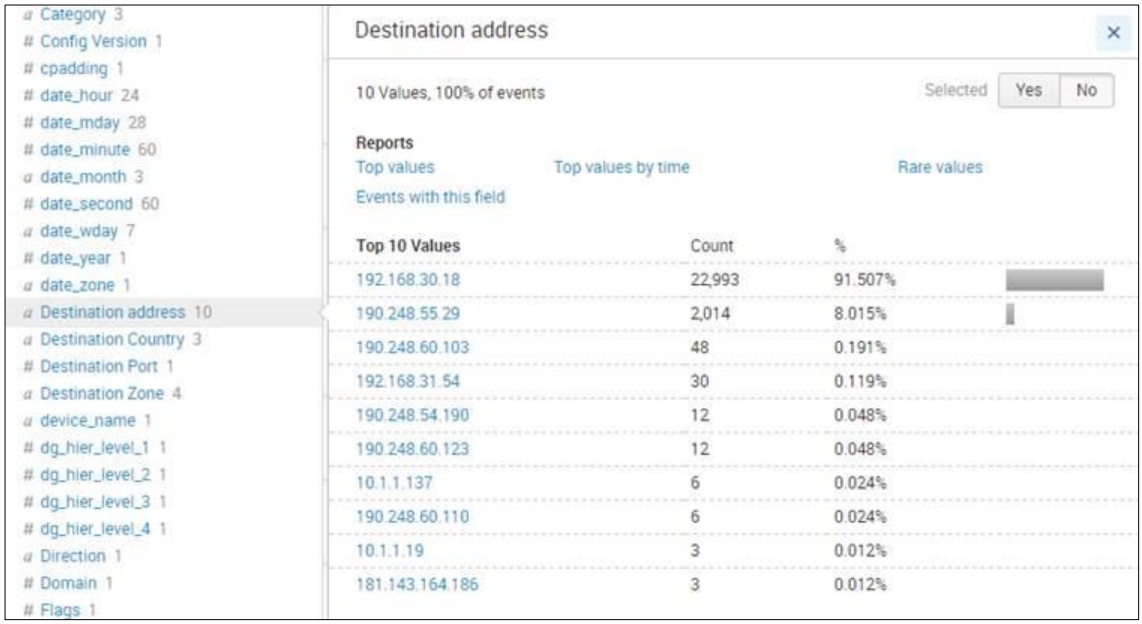
Gráfica 7. Países de origen que activaron la firma *HTTP SQL Injection Attempt* (36239)



Fuente: Logs NGFW CAN diciembre de 2016.

En la gráfica 8, se observa el direccionamiento destino relacionado con la firma *HTTP SQL Injection Attempt* (36239), donde se detalla la dirección IP, cantidad de tráfico y su porcentaje; estos datos permiten detectar cual es el servidor que está recibiendo este tipo de tráfico y posteriormente validar a nivel de host, los logs a nivel de aplicación, eventos del antivirus local, script defacement, entre otros. Como resultado se determinará si el servidor fue comprometido y si está asociado a la firma detectada.

Gráfica 8. Direccionamiento destino a la que va dirigido el tráfico con la activación de la firma *HTTP SQL Injection Attempt* (36239)



Fuente: Logs NGFW CAN diciembre de 2016.

En el cuadro 8, se relacionan las URLs asociadas a las IPs detectadas en la gráfica 8, el cual es un insumo importante para la sustentación del RFC, donde el cliente conociendo la lógica de la entidad y la criticidad de la aplicación (ver numeral 15), aprueba o deniega la solicitud de bloqueo de esta firma.

Cuadro 9. Relación de la identificación de las páginas con el direccionamiento de la firma *HTTP SQL Injection Attempt* (36239)

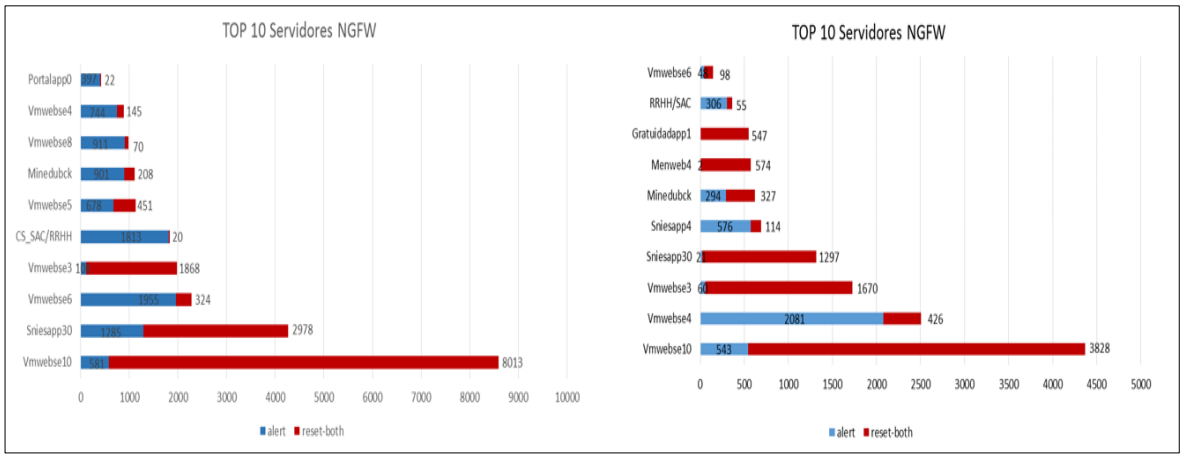
HTTP SQL Injection Attempt (36239)		
Porcentaje	**IP**	**URL**
91,5%	192.168.30.18	http://documentacion.mineducacion.gov.co/mengesdoc/validacion.asp
8,0%	190.248.55.29	http://documentacion.mineducacion.gov.co/mengesdoc/validacion.asp
0,2%	190.248.60.103	menapp1.minedu.gov.co
Fuente: Logs NGFW DIVEO diciembre de 2016 y CMDB.		

Como conclusión, se observa en la gráfica 8, que el país o red origen que activó la firma *HTTP SQL Injection Attempt* (36239) es en primer lugar el segmento de red 172.16.X.X correspondiente a red interna Colombia Compra Eficiente con el 89.5%, en segundo Colombia con el 9,7% y en tercer lugar Turquía con el 0,1%, por lo que se concluye que gran parte del tráfico generado hace parte de consultas del interior del país, por lo que hay altas probabilidades que sea un falso positivo, de igual manera se sugiere el bloqueo de esta firma con el objetivo de preservar la integridad, confidencialidad y disponibilidad de los aplicativos que contienen las URLs descritos en el cuadro 9, adicionalmente se sugiere que si luego de activar el bloqueo de las firmas llegase a presentarse un bloqueo a nivel de funcionalidad se cree una exclusión específica indicando la IP origen y destino, pero sin desactivar el bloqueo de la firma.

18.2 TOP 10 SERVIDORES CON MÁS EVENTOS – DIVEO Y CAN

Las gráficas denominadas “Top 10 servidores con más eventos” del anexo C, permiten visualizar cuales son los 10 servidores con más transferencia de tráfico, discriminando entre el tráfico bloqueado (color rojo) y el permitido (color azul), por ejemplo, en la gráfica 9 se observa el top 10 de servidores con más eventos, donde la gráfica de la izquierda corresponde al mes de mayo y la gráfica de la derecha al mes de diciembre. Para el mes de mayo se puede observar que servidor vmwebse10 se encuentra aproximadamente 90% bloqueado, cabe destacar que sobre este servidor se publican alrededor de 50 páginas de las secretarias a nivel nacional y para el mes de diciembre y sobre los servidores vmwebse3 y sniesapp30 se encuentran a más del 90% con el trafico bloqueado, este tipo de información permite enfocar el análisis de logs en los dispositivos NGFW y WAF basados en la premisa que si alguna aplicación es objetivo de ataque se traduce en mayor tráfico bloqueado debido a los múltiples intentos para explotar una vulnerabilidad, adicionalmente es un insumo para validar en otra capa de seguridad, como revisar directamente sobre el servidor a nivel de antivirus local, logs en la aplicación, script defacement entre otros.

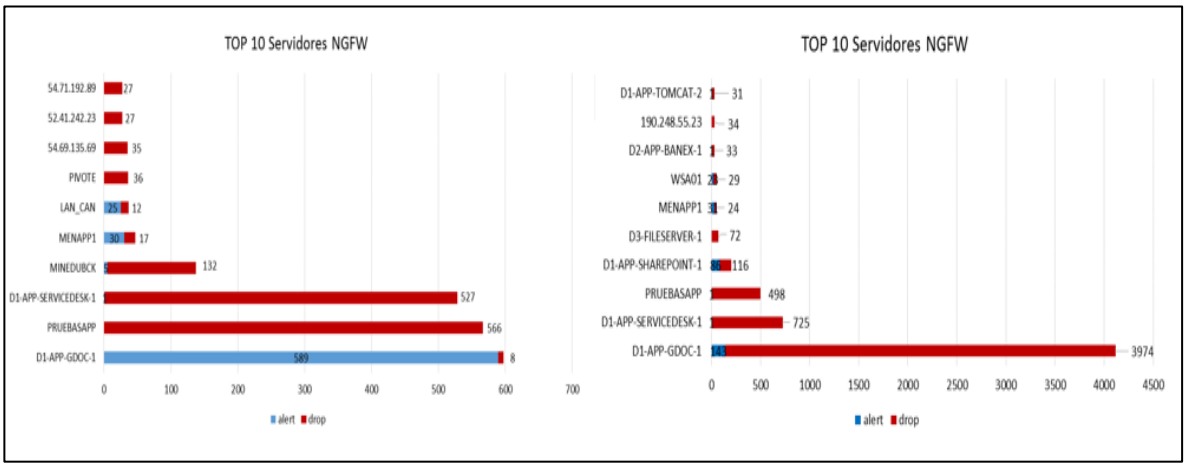
Gráfica 9. Top 10 Servidores con más eventos Mayo vs Diciembre – DIVEO



Fuente: Logs NGFW DIVEO mayo y diciembre de 2016.

La gráfica 10 que corresponde a la sede de CAN, se observa que en el mes de mayo para servidor D1-APP-GDOC-1 contaba con aproximadamente 98% de tráfico permitido mientras que para el mes de diciembre contaba con aproximadamente 95% de tráfico bloqueado, lo que permite inferir que este comportamiento es debido al incremento de bloqueo de firmas desde el mes de mayo al mes de diciembre, aumentando la contención de amenazas.

Gráfica 10. Top 10 Servidores con más eventos Mayo vs Diciembre – CAN



Fuente: Logs NGFW DIVEO mayo y diciembre de 2016.

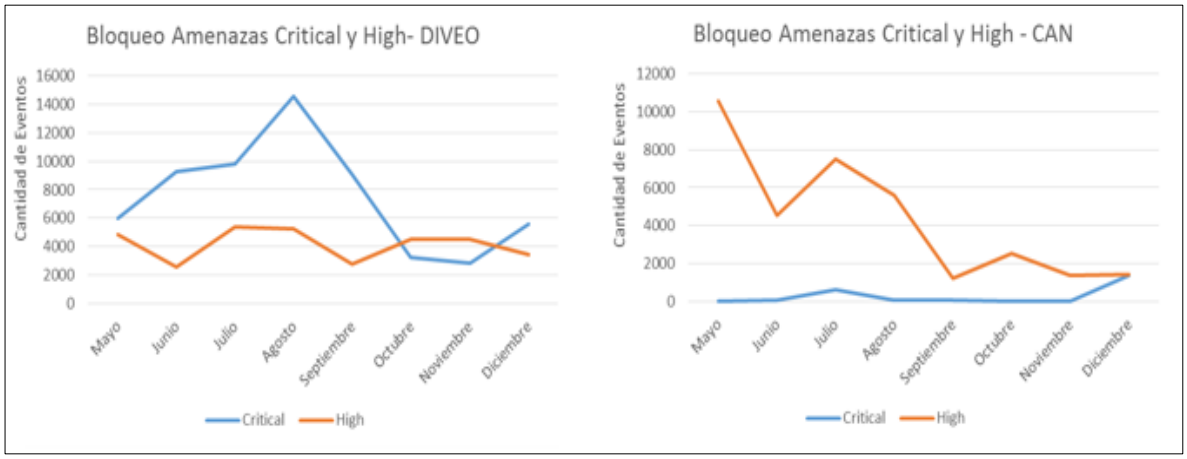
18.3 RESUMEN BLOQUEO POR SEVERIDAD *CRITICAL* Y *HIGH* – DIVEO Y CAN

Las gráficas 11 y 12 consolidan la cantidad de firmas bloqueadas en el módulo amenazas con severidad *critical y high* desde el mes de mayo a diciembre, las cuales permiten:
Dar a conocer al cliente las contenciones que están realizando los NGFW sobre las amenazas con severidad *critical y high*, de tal manera que se pueda visualizar la efectividad de detección de estos dispositivos.

Observar el comportamiento de la cantidad de bloqueo de severidad *critical* y *high* para cada uno de los meses, el cual será un insumo de análisis para los picos que se presenten en las gráficas 11 y 12, debido a que se puede estar presentando una amenaza específica o estar en presencia de un APT (*Advanced Persistent Threat).*

En general las gráficas 11 y 12 presentan una tendencia de disminución de bloqueos de las amenazas con severidad *crítical* y *high*, lo cual es positivo ya que el MEN disminuye la percepción de ataque para estas severidades, pero no se puede dejar de lado el análisis de logs ya que sería una “falsa expectativa de seguridad”.

Gráfica 11. Resumen bloqueo de amenazas *Critical* y *High* para DIVEO y CAN

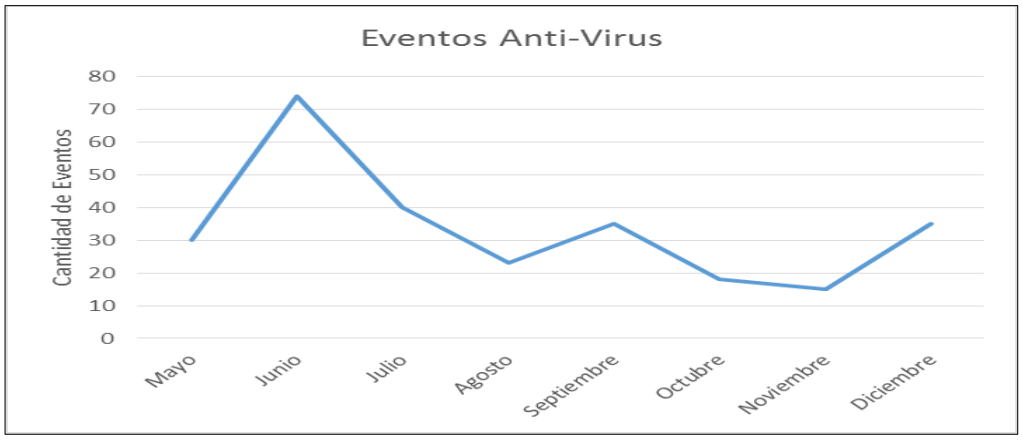


Fuente: Logs NGFW DIVEO y CAN.

18.4 RESUMEN ANTI-VIRUS - CAN

En la gráfica 12, se observa que los eventos a nivel anti-virus oscilan entre 12 y 75 eventos, lo cual no es una cifra significativa y con una tendencia a la baja. Es importante resaltar que el 100% de este módulo se encuentra bloqueado.

Gráfica 12. Resumen de eventos registrados en el módulo anti-virus – CAN

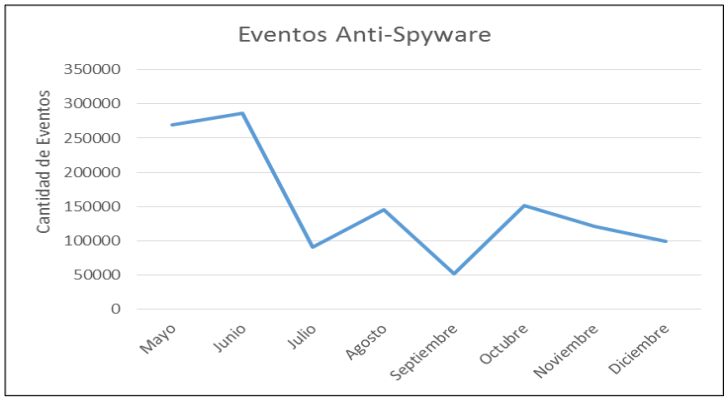


Fuente: Logs NGFW CAN.

18.5 RESUMEN ANTI-SPYWARE - CAN

En la gráfica 13, se evidencia que los eventos a nivel de anti-spyware oscilan entre 50000 y 290000, una gran cantidad de eventos, con una tendencia a la baja para el período comprendido a partir del mes de mayo al mes de diciembre. Para este módulo fue de gran importancia el análisis que se llevó a cabo en el anexo B, ya donde la gran mayoría de detecciones fueron por *spyware*, el cual sirvió de soporte para solicitar el bloqueo de las severidades *high*, *medium* y *low*. El bloqueo se llevó a cabo en las severidades *high* y *medium* en el mes de junio por la gran cantidad de spyware que estaba detectando por medio del correo; y la severidad *low* fue bloqueada en el mes de diciembre como se puede corroborar en el anexo C.

Gráfica 13. Resumen de eventos registrados en el módulo Anti-Spyware – CAN



Fuente: Logs NGFW CAN.

18.6 EVENTOS WILDFIRE

Como se describió en el numeral 8.4.1.1 llamado prevención de amenazas, el módulo de Wildfire es propiedad de NGFW, el cual realiza un análisis en la nube para la identificación de malware conocido o desconocido (día cero) clasificándolo como Malware, Greyware y Benign.

Luego de la inspección y análisis de los eventos registrados en Wildfire que se detallan en el anexo C, se identificó que los eventos categorizados como malware correspondían efectivamente a virus, gusanos, troyanos, herramientas de acceso remoto (RAT), rootkits y botnets, por tal motivo fue solicitado formalmente el bloqueo de la categoría malware en los NGFW en la sede CAN, en la sede de DIVEO no se tenía registros de eventos en este módulo, pero de igual manera se sugirió como acción preventiva el bloqueo de Wildfire para la categoría de Malware.

Los eventos categorizados como greyware en los NGFW del CAN, fueron un gran aporte para analizar tráfico sospechoso o anómalo en la red del MEN.

18.7 RESUMEN GRÁFICAS WAF

Las gráficas estadísticas de los dispositivos WAF que se encuentran en el anexo C, más que ser un insumo de referencia para realizar afinamiento de seguridad sobre el dispositivo, sirvió como indicador de consumo de acceso para las gráficas categorizadas como “Top de amenazas por firmas” y “Top sitios web con más eventos”, el motivo es porque al llevar a cabo el análisis de las firmas que se

encontraban permitidas en las categorías de gráficas mencionadas, se identificó que cada firma se encontraba relacionada con la mayoría de las aplicaciones por lo que el bloqueo de alguna de las firmas generaría indisponibilidad del servicio y por este motivo fueron catalogadas como falsos positivos.

De acuerdo a lo anteriormente descrito se llevó a cabo un análisis de las firmas que no se encontraban en las gráficas categorizadas como “Top de amenazas por firmas” y “Top sitios web con más eventos”, por lo que las firmas bloqueadas a nivel de WAF se pueden visualizar en el anexo C en la categoría llamada “Top bloqueo por firmas”.

Para los dispositivos de WAF NetScaler se quiere resaltar lo descrito en el numeral 12.2, donde la empresa de consultoría e investigación Gartner describe que la función principal de los NetScaler es de ADC como balanceador y optimizador de tráfico y que la solución de WAF es una característica adicional, y por tal motivo es que en el cuadrante mágico de Gartner se encuentra ubicado entre los últimos en el nicho de competidores, adicionalmente Gartner tiene las siguientes observaciones frente a la solución de WAF NetScaler:

- Los clientes existentes reportan frustración con las funciones de registro y generación de informes.
- La tendencia de ventas en los últimos meses a nivel de solución de WAF ha sido desplazada por sus competidores.
- Gartner no ve el WAF de Citrix desplazando a la competencia basada en sus capacidades de seguridad, sino que la ve como una venta complementaria para las soluciones de ADC.

19. INCIDENTES DE SEGURIDAD

En el anexo D, se describen 2 incidentes denominados Website Defacement presentados sobre dos páginas del MEN (semgirardot y saces-pares), los días 8 de junio y 22 de julio de 2016, en lo que se pudo identificar la IP del atacante y con esta IP se procedió a validar el registro de eventos en los dispositivos NGFW y WAF de DIVEO, encontrando lo siguiente, para cada dispositivo respectivamente:

NGFW:

- En el ataque del 8 de junio de 2016, la IP del atacante correspondía por geolocalización a una IP *"Anonymous proxy"* y al revisar en el NGFW se observó que activó la firma llamada PHP Remote File Inclusion Vulnerability (33336) catalogada como severidad medium y estaba siendo alertada, es decir, el dispositivo estaba permitiendo el tráfico de esta firma, por lo que se recomendó como control correctivo el bloqueo de la firma.
  Como insumo de apoyo nos remitimos al resultado de escaneo de vulnerabilidades específicamente para este servidor y encontramos que la versión de PHP se encontraba desactualizada y sin soporte, debido a que contaba con la versión 4.4 y la versión estable y sugerida en ese periodo era la 5.3 la clasificación de severidad para esta vulnerabilidad es critical.
- En el ataque del 22 de julio de 2016, la IP del atacante correspondía por geolocalización a una IP "Ucrania" y al revisar en el NGFW se observó que activó la firma WordPress Login BruteForce Attempt (40044) catalogada como severidad critical y estaba siendo bloqueada; debido a que se encontraba bloqueada se procedió a revisar en el módulo de tráfico evidenciando múltiples registros hacia la página comprometida con paquetes del mismo tamaño, por lo que se concluyó que estaba realizando un ataque de fuerza bruta, lamentablemente en la base de datos de firmas de amenazas del NGFW no se encontraba una firma relacionada con este tráfico o no estaba relacionado con la firma de ID 40444.

De acuerdo a la no identificación de una o varias firmas en el ataque del 22 de julio en los dispositivos NGFW de la materialización de este ataque, se trae como referencia un párrafo de un documento indexado IEEE llamado "A Knowledge-Based Approach To Intrusion Detection Modeling", la cual describe:

> "State of the art intrusion detection and prevention system (IDPS) perform signature-based monitoring of the cyber-infrastructure to identify any malicious activities and generate an alert when such activities are detected. These

systems share a limitation that if the signature of an attack is not available in there database, they cannot detect it"[47].

WAF:

En la revisión de estos 2 incidentes sobre el WAF no se evidencio la activación de ninguna firma.

[47] IEEEXplore. A. Knowledge-Based Approach to Intrusion Detection Modeling], [consultado el 5 de enero de 2017]. Disponible en: http://ieeexplore.ieee.org/document/6227687/

20. RECOMENDACIONES NGFW y WAF

Teniendo presente que uno de objetivos específicos de este proyecto es proporcionar recomendaciones para la adquisición o renovación de los dispositivos NGFW y WAF, de acuerdo a los resultados de detección, contención de amenazas y malware con las marcas Palo Alto Netwoks para el NGFW y NetScaler Citrix para el WAF, se tienen las siguientes observaciones:

20.1 NGFW PALO ALTO NETWORKS

Los resultados de detección de amenazas y malware en los dispositivos NGFW en las sedes de CAN y DIVEO permitieron generar en el trascurso de este proyecto un gran número de bloqueos de firmas y módulos (ver numerales 17, 18.1-6 y 19), generando confianza al cliente a nivel de seguridad perimetral. También hay que destacar que la solución de registros de logs se encuentra en el mismo dispositivo y no alojado en un servidor externo lo que me permitió como analista de los eventos y alarmas una gran eficiencia, efectividad y rapidez en la parametrización de los mismos, facilitando el rastreo de amenazas y así mismo proponer de manera temprana controles preventivos y correctivos. De acuerdo a lo anteriormente descrito la recomendación a la fecha es continuar con la solución NGFW de la marca Palo Alto Networks, respaldado también con el posicionamiento que tiene en el cuadrante mágico de Gartner ubicándolo como líder (ver numeral 12.1).

20.2 WAF NETSCALER CITRIX

Con base a las deficiencias que se han evidenciado en los WAF NetScaler Citrix (ver numerales 18.7 y 19), se propone el dispositivo Imperva debido, a la relación costo/beneficio y a su posición dentro del cuadrante mágico de Gartner que lo ubica como único líder en este segmento (ver numeral 12.2), a continuación, se describe alguna de las características tomadas de Gartner:

Imperva es evaluado como líder porque se destaca continuamente frente a sus competidores en características e innovaciones de seguridad, proporcionando detección precisa de las amenazas y con precios competitivos respecto a sus competidores directos. Imperva es un candidato fuerte para cualquier organización, especialmente para aquellas que busquen requisitos de alta seguridad o aquellas que busquen un WAF basado en la nube de fácil implementación[48].

[48] GARTNER, Magic Quadrant for Web Application Firewalls. [En línea], [consultado el 5 enero de 2016]. Disponible en: https://www.gartner.com/doc/reprints?id=1-3BZK2PZ&ct=160720&st=sb

21. CONCLUSIONES

Al finalizar el proyecto de grado donde se analizaron y valoraron los eventos y alarmas de los dispositivos NGFW de Palo Alto Netwoks y WAF de NetScaler, apoyados en la valoración de equipos, escaneo de vulnerabilidades, arquitectura, permisos de firewall, categorización según la criticidad de los activos de información y reportes estadísticos mensuales se llegaron a las siguientes conclusiones:

- De acuerdo a la arquitectura de red se observa que no se llevó a cabo una valoración inicial para la adquisición de los NGFW debido a que se evidencio redundancia innecesaria sobre estos dispositivos.

- El conocimiento previo de las aplicaciones críticas del MEN determinadas por el cliente, fue un insumo importante para filtrar, priorizar los eventos y alarmas de los dispositivos NGFW y WAF.

- Al analizar y estudiar la arquitectura de red, zonas, direccionamiento y permisos de firewall, permitió determinar y asociar de manera global el flujo de tráfico y las posibles amenazas a los que podrían estar expuestas las aplicaciones publicadas, privilegios sobre los servidores desde el área de TI y direccionamiento correspondiente a los servidores de pruebas, desarrollo y producción.

- Al analizar y estudiar la arquitectura de red en la sede CAN, se llegó a la conclusión que la ubicación del dispositivo del NGFW no tenía visibilidad de los endpoints en la LAN, por lo que se decidió configurar un modo TAP el dispositivo NGFW conectado directamente al switch core.

- Al analizar y estudiar las zonas, direccionamiento y permisos de firewall de la sede DIVEO se evidenció que los módulos de anti-virus y anti-spyware no estaban registrando eventos debido a que se tenían fuertes políticas de acceso.

- El resultado de escaneo de vulnerabilidades en conjunto con los permisos de acceso a nivel de firewall perimetral encaminó el análisis de eventos y alarmas en los dispositivos NGFW y WAF, ya que se tenían presente las vulnerabilidades que podían ser explotadas de acuerdo a los permisos.

- El valorar los dispositivos NGFW y WAF conociendo las fortalezas y debilidades de cada solución apoyados en los argumentos de la empresa de consultoría Gartner, ubicando los NGFW de Palo Alto Netwoks como líderes en este segmento y con los resultados de detección de amenazas y malware

plasmados en este proyecto de investigación permitió presentar al cliente de manera formal el bloqueo varias firmas y categoría de los módulos de este dispositivo. En cambio, los resultados que se obtuvieron con el análisis de eventos y gráficas del WAF NetScaler no fueron los esperados, los cual fueron anticipados por Gartner, indicando que su característica principal es el balanceo de carga y que la solución de WAF es un valor agregado. Efectivamente estos dispositivos se están utilizando como balanceadores en el MEN y a nivel de WAF se pudieron realizar solo algunos bloqueos de firmas.

- Las gráficas mensuales con base a los eventos y alarmas detectadas por los dispositivos NGFW y WAF permitieron medir porcentualmente y cuantitativamente el top de amenazas y malware permitidas y bloqueadas, siendo un insumo para realizar el análisis de las firmas permitidas y evidenciar el nivel de contención de los dispositivos en caso de bloqueos.

- Se evidencio que los PCs infectados con spyware fue causado por que no se tenía una gestión apropiada del antivirus Kaspersky, el cual hace parte de la responsabilidad del MEN.

- Luego del afinamiento realizado en los dispositivos NGFW que se llevó a cabo en el trascurso de la elaboración del proyecto de grado, se observó una disminución en la materialización de incidentes de seguridad.

BIBLIOGRAFÍA

ALEGSA.COM. Definición de vulnerabilidad. [En línea], [consultado el 23 de abril de 2016]. Disponible en: http://www.alegsa.com.ar/Dic/vulnerabilidad.php.

AMUTIO, Miguel. MAGERIT. Versión 3. España: Dirección General de Modernización Administrativa. 2012, p.9.

CISCO, Glossary, [En línea] [consultado el 28 de noviembre de 2016]. Disponible en: http://www.cisco.com/c/en/us/td/docs/security/asa/asa80/configuration/guide/conf_gd/glossary.html#wp1022456.

CITRIX. Citrix Glossary. [En línea], [consultado el 28 de noviembre de 2016]. Disponible en: https://www.citrix.com/glossary/.

CISCO. Chapter: Configuring SSIDs. [En línea] [consultado el 5 de marzo de 2016]. Disponible en: http://www.cisco.com/c/en/us/td/docs/wireless/access_point/1300/12-2_15_JA/configuration/guide/o13ssid.html. Traducción autor.

CISCO. Chapter: Understanding and Configuring VLANs. [En línea], [consultado el 5 de marzo de 2016], Disponible en: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/25ew/configuration/guide/conf/vlans.html. Traducción autor.

CISCO. Configuring DMZ. [En línea], [consultado el 5 de marzo de 2016]. Disponible en: https://www.cisco.com/assets/sol/sb/isa500_emulator/help/guide/ad1681599.html. Traducción autor.

CITRIX, Configuring the Application Firewall. [En línea], [consultado el 5 junio de 2016]. Disponible en: http://docs.citrix.com/en-us/netscaler/11/security/application-firewall/configuring-application-firewall.html.

CROTHERS, Tim. Implementing Intrusion Detection System. Indianápolis, Wiley publishing, Inc., 2003, p.10.

DoS, DENIAL OF SERVICE. Ataque por denegación de servicio. [En línea], [consultado el 23 de abril de 2016]. Disponible en: http://es.ccm.net/contents/22-ataque-por-denegacion-de-servicio.

GARTNER, IT Glossary. [En línea] [Consultado el 29 de noviembre de 2016] Disponible en: http://www.gartner.com/it-glossary/next-generation-firewalls-ngfws MATT, Walker, CEH. 2 ed. United Sates: American Express, 2014, p.386.

IEEEXplore. A Knowledge-Based Approach to Intrusion Detection Modeling.], [En línea], [Consultado el 5 de enero de 2017]. Disponible en: http://ieeexplore.ieee.org/document/6227687.

ITU. Techniques for preventing web-based attacks. [En línea], [consultado el 28 de noviembre de 2016]. Disponible en: http://www.itu.int/itu-t/recommendations/rec.aspx?rec=12154.

KRUEGEL, Christopher. VALEUR, Fredrik. VIGNA, Giovanni. Intrusion Detection and Correlation, Volumen 14, Springer US, 2005, p.17. Traducción autor.

MATT, Walker, CEH. 2 ed. United Sates: American Express, 2014. p.403
McAfee. Glosario. [En línea] [Consultado el 23 de noviembre de 2016]. Disponible en: https://home.mcafee.com/virusinfo/glossary#H.

MINISTERIO DE EDUCACIÓN. Lineamientos técnicos y administrativos. [En línea], [consultado el 23 de abril de 2016]. Disponible en: http://www.mineducacion.gov.co/1759/w3-article-89266.html.

OWASP. Aplicación Firewall. [En línea], [consultado el 23 de abril de 2016]. Disponible en: https://www.owasp.org/index.php/Web_Application_Firewall&prev=search.

PALO ALTO NETWORK. IPS. [En línea], [consultado el 25 de noviembre de 2016]. Disponible en: https://www.paloaltonetworks.com/products/secure-the-network/next-generation-firewall.

PALO ALTO NETWORK. IPS. [En línea], [consultado el 24 de noviembre de 2016]. Disponible en: https://www.paloaltonetworks.com/features/ips.

PALO ALTO NETWORK. IPS para empresas. [En línea], [consultado el 23 de noviembre de 2016]. Disponible en: https://www.paloaltonetworks.com/documentation/70/pan-os/pan-os/networking/interface-deployments.

PALO ALTO NETWORK. IPS para empresas. [En línea], [consultado el 23 de noviembre de 2016]. Disponible en: https://www.paloaltonetworks.es/products/features/ips.html.

PALO ALTO NETWORK. IPS. [En línea], [consultado el 24 de noviembre de 2016]. Disponible en: https://www.paloaltonetworks.com/features/ips.

PALO ALTO NETWORK. Intrusion Detection System - IDS technology and deployment. [En línea], [consultado el 23 de noviembre de 2016]. Disponible en: https://www.paloaltonetworks.com/documentation/glossary/what-is-an-intrusion-detection-system-ids.

Registrada por la comunidad de la oficina de comercio del Gobierno de Inglaterra. ITIL FUNDAMENTOS DE ADMINISTRACIÓN DE SERVICIOS. Versión 5. United States: FoxIT, 2011. p.21 y 29.

SANS. Glossary of Security Terms. [En línea] [Consultado el 23 de noviembre de 2016]. Disponible en: https://www.sans.org/security-resources/glossary-of-terms/.

SONICWALL. Soluciones de administración unificada. [En línea], [consultado el 23 de abril de 2016]. Disponible en: http://www.sonicwall.com/mx-es/solutions/unified-threat-management/.

SEGURIDAD INFORMÁTICA. Amenazas a la seguridad de la información. [En línea], [consultado el 23 de abril de 2016]. Disponible en: http://www.seguridadinformatica. unlu.edu.ar/?q=node/12.

SHON, Harris. CISSP. 6 ed. United States: American Express, 2013, p.1383.

SHON, Harris. CISSP. 6 ed. United States: American Express, 2013, p.23.

SHON, Harris. CISSP. 6 ed. United States: American Express, 2013, p.27.

STALLINGS, William Lawrie brown. Computer Security Principles and practices. (Base RFC7474) traducción, p.18.

VID INFO. 5 avanzadas persistentes amenazas APT. [En línea], [consultado el 23 de abril de 2016]. Disponible en: http://media.kaspersky.com/documents/ business / brfwn/ en/ Advanced-persistent-threats-not-your-average-malware_ Kaspersky-Endpoint-Control-white-paper.pdf.

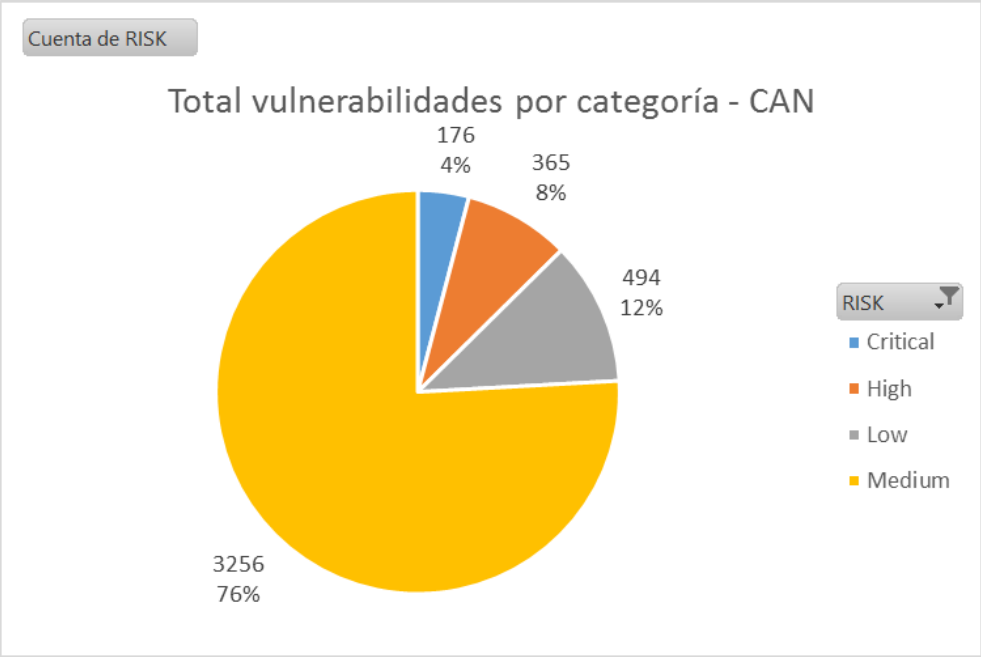
WSP-CONSULTING. Request for Change (RFC). [En línea] [Consultado el 29 de noviembre de 2016] Disponible en: https://wsp-consulting.de/SM_help/content/glossary/request_for_change_rfc.htm.

ANEXOS

ANEXO A. RESULTADO DEL ESCANEO DE VULNERABILIDADES

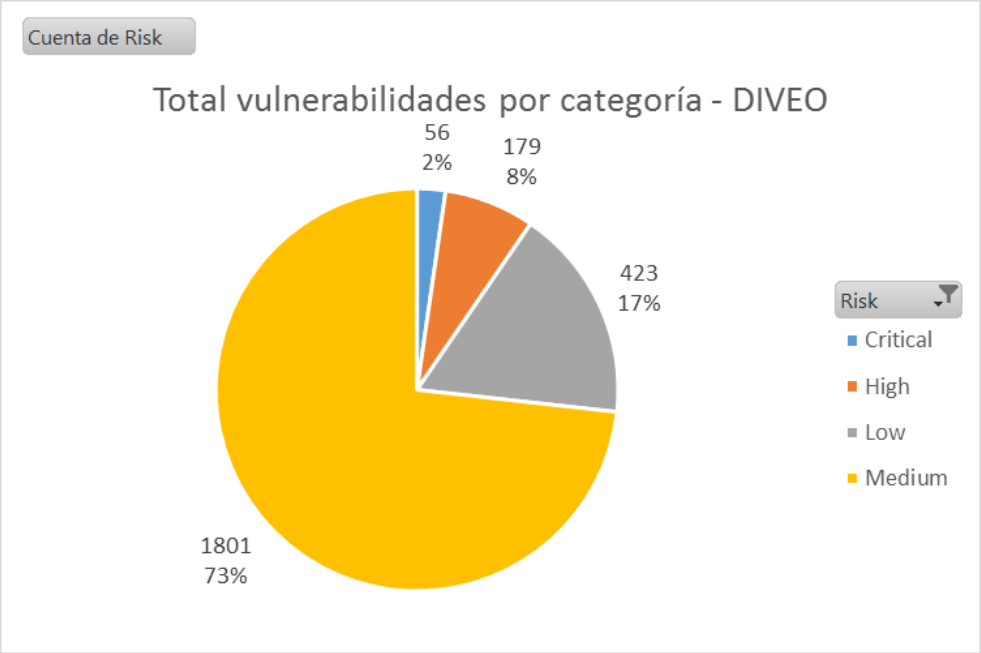
En los segmentos de red escaneados, se analizaron en total 257 servidores en DC CAN y 434 servidores en DC DIVEO, identificando entre vulnerabilidades *low*, *medium*, *high* y *critical*, 4291 en DC CAN y 2459 vulnerabilidades en DC DIVEO como se observa en las gráficas 14 y 15:

Gráfica 14. Total de vulnerabilidades por categoría – CAN



Fuente: Reporte de Nessus.

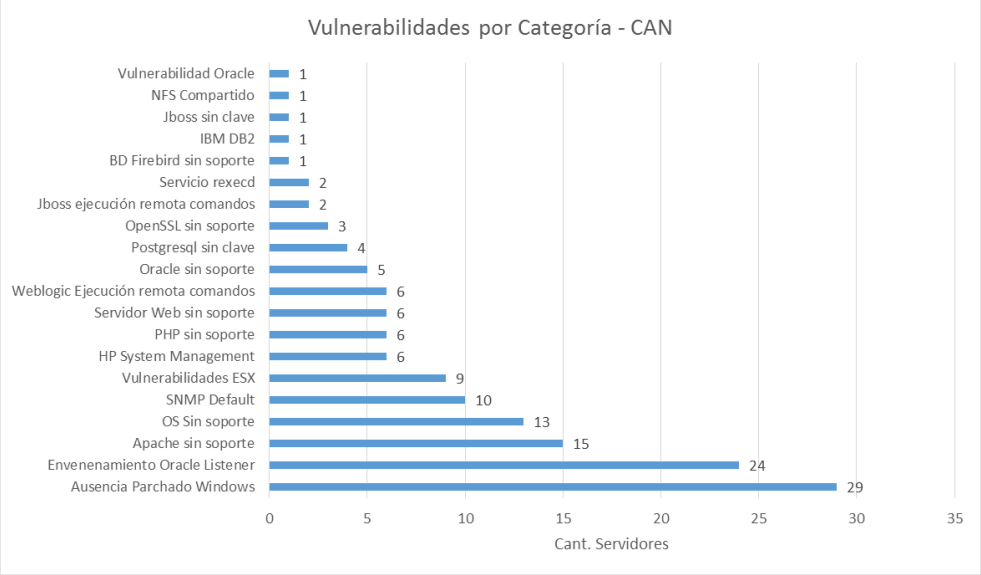
Gráfica 15. Total vulnerabilidades por categoría - DIVEO



Fuente: Reporte de Nessus.

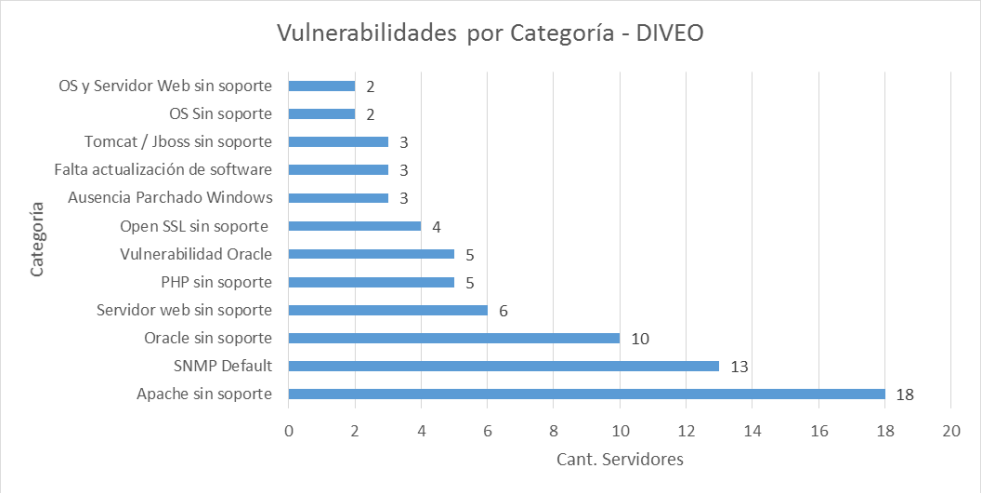
En las gráficas 16 y 17 se observa la categorización de las vulnerabilidades con severidad "*Critical*" y "*high*" para las sedes de CAN y DIVEO respectivamente:

Gráfica 16. Vulnerabilidades por categoría – CAN



Fuente: Categorización del reporte de Nessus.

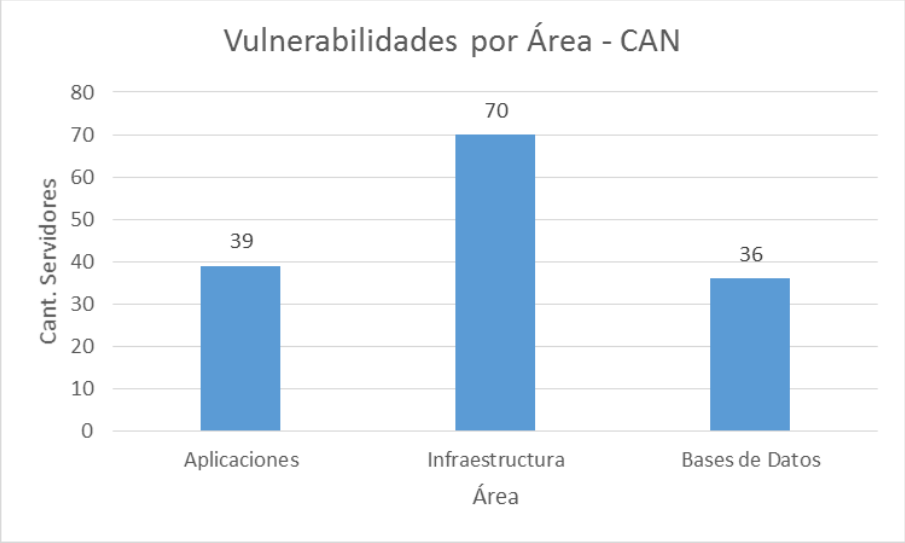
Gráfica 17. Vulnerabilidades por categoría - DIVEO



Fuente: Categorización del reporte de Nessus.

En la gráfica 18 se observa la relación de cantidad de vulnerabilidades y el área responsable para su revisión y mitigación en la sede del CAN:

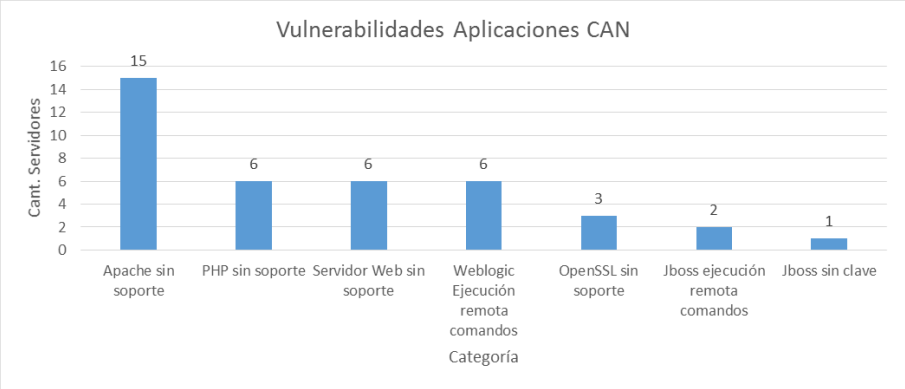
Gráfica 18. Vulnerabilidades por área – CAN



Fuente: Relación por área del reporte de Nessus.

El área de aplicaciones para la sede del CAN tiene asociadas 39 vulnerabilidades y en la gráfica 19 se da a conocer a que corresponden, identificando el nombre y la cantidad:

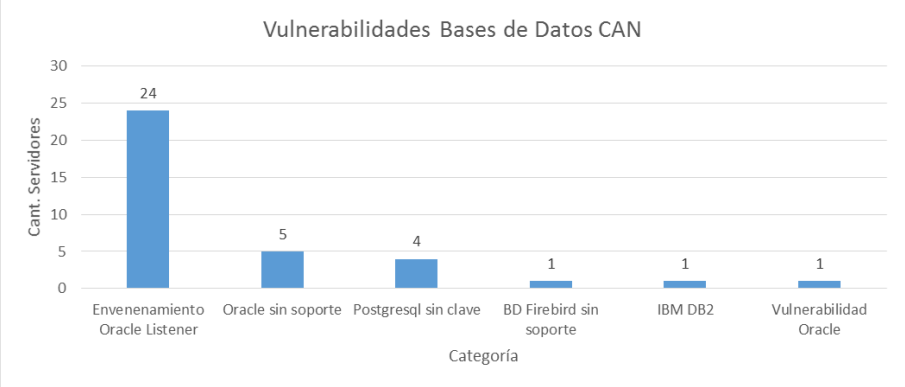
Gráfica 19. Vulnerabilidades aplicación – CAN



Fuente: Reporte de Nessus.

Igualmente en la gráfica 18, el área de bases de datos para la sede del CAN tiene asociadas 36 vulnerabilidades y en la gráfica 20 se da a conocer a que corresponden, identificando el nombre y la cantidad:

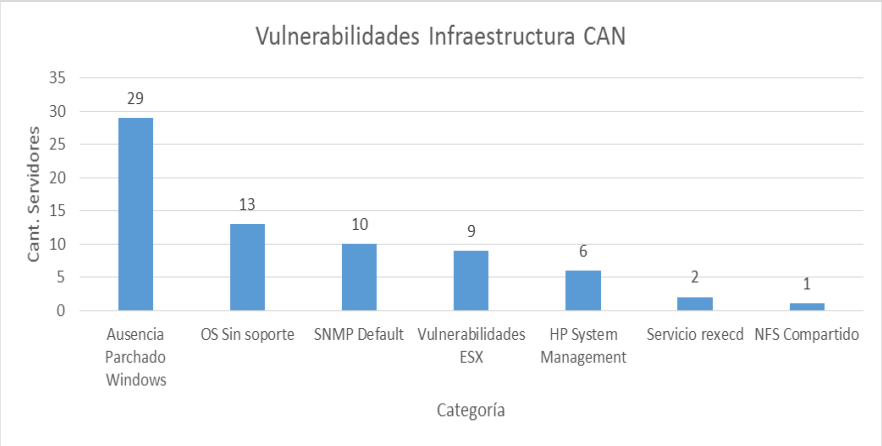
Gráfica 20. Vulnerabilidades bases de datos – CAN



Fuente: Reporte de Nessus.

Como se observa en la gráfica 18, el área de infraestructura para la sede del CAN tiene asociadas 70 vulnerabilidades y en la gráfica 21 se da a conocer a que corresponden, identificando el nombre y la cantidad:

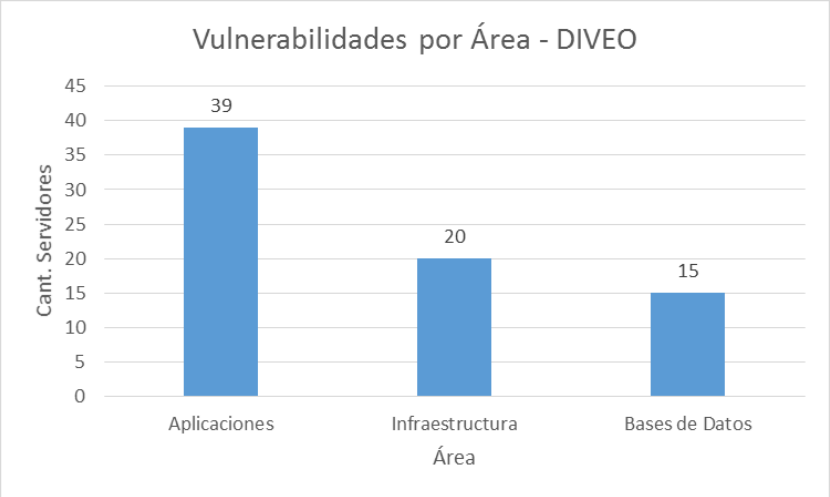
Gráfica 21. Vulnerabilidades infraestructura – CAN



Fuente: Reporte de Nessus.

En la gráfica 22 se observa la relación de cantidad de vulnerabilidades y el área responsable para su revisión y mitigación en la sede de DIVEO:

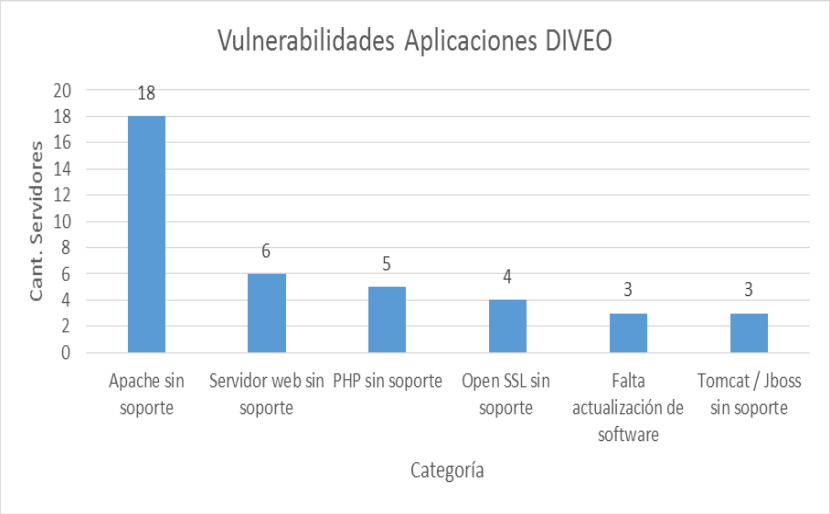
Gráfica 22. Vulnerabilidades por área - DIVEO



Fuente: Reporte de Nessus.

El área de aplicaciones para la sede de DIVEO tiene asociadas 39 vulnerabilidades y en la gráfica 23 se da a conocer a que corresponden, identificando el nombre y la cantidad:

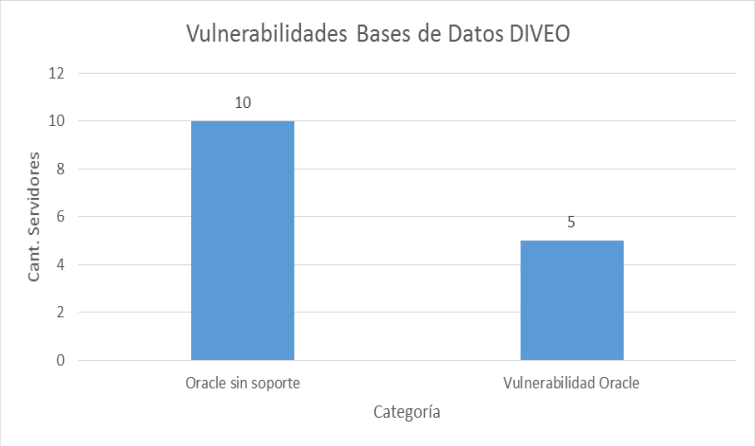
Gráfica 23. Vulnerabilidades aplicaciones – DIVEO



Fuente: Reporte de Nessus.

Igualmente en la gráfica 22, el área de bases de datos para la sede de DIVEO tiene asociadas 15 vulnerabilidades y en la gráfica 24 se da a conocer a que corresponden, identificando el nombre y la cantidad:

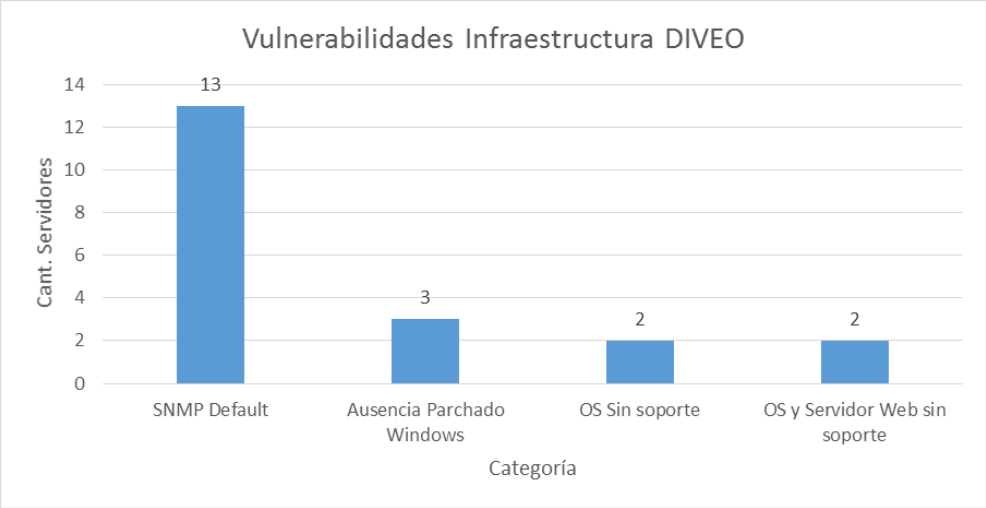
Gráfica 24. Vulnerabilidades bases de datos – DIVEO



Fuente: Reporte de Nessus.

Como se observa en la gráfica 22, el área de infraestructura para la sede de DIVEO tiene asociadas 20 vulnerabilidades y en la gráfica 25 se da a conocer a que corresponden, identificando el nombre y la cantidad:

Gráfica 25. Vulnerabilidades infraestructura – DIVEO



Fuente: Reporte de Nessus.

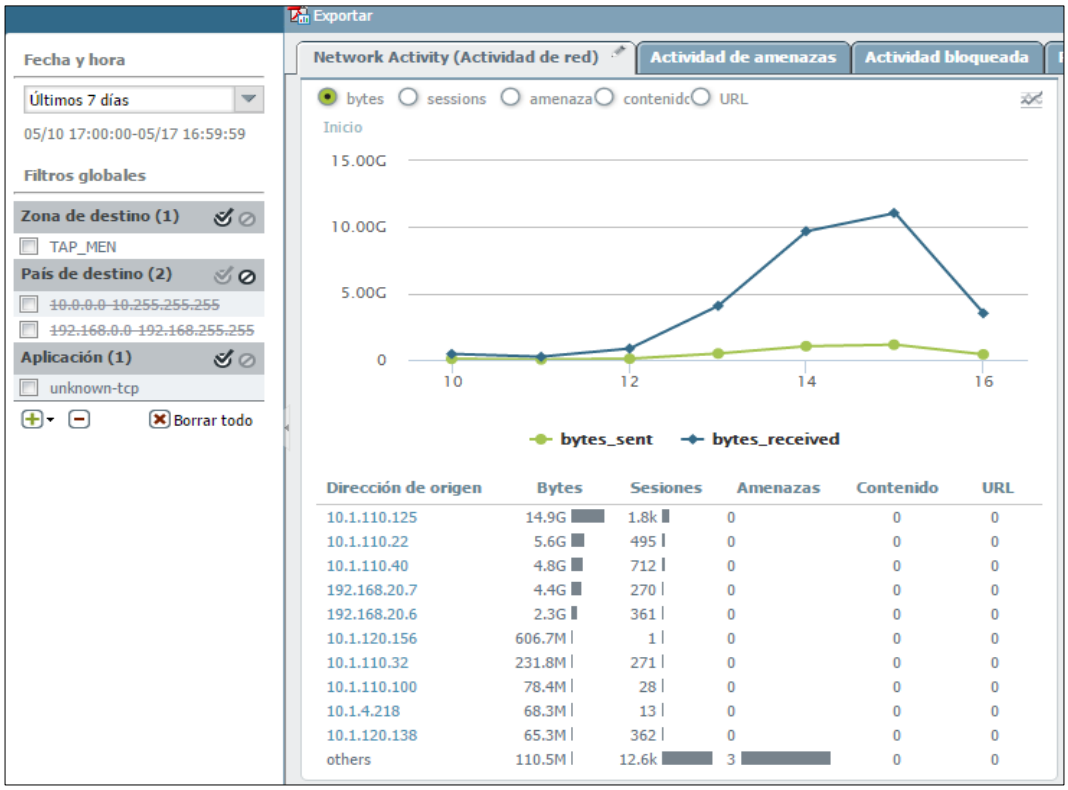
ANEXO B. ANÁLISIS DE TAP

A continuación, se dará a conocer a nivel cronológico los correos enviados al Asesor de Seguridad del MEN para que lleve el control correctivo de los eventos de *malware*:

- **Detección de amenaza miércoles 18/5/2016**

Me permito informar que se identificó el uso de aplicaciones para saltar los bloqueos de acceso a internet que se tienen por defecto (pornografía y sitios de hacking), dejando únicamente registró en los dispositivos de seguridad como tráfico TCP DESCONOCIDO, tal como se observa en la figura 12:

Figura 12. Detección de amenaza miércoles 18/5/2016



Fuente: *Dashboard* NGFW CAN.

Las direcciones IP que generan la mayor cantidad de tráfico desconocido coinciden con direcciones IP que estaban consumiendo servicios de TOR, como la 10.1.110.125 y 10.1.110.40. (Nota: la IP 10.1.120.156 corresponde al especialista

de une que estaba probando el software para saltar las restricciones y por eso aparece en el registro).

Teniendo en cuenta que el uso reiterado de mecanismos para saltar las restricciones de navegación, atentamente solicitamos al MEN que se tome una decisión sobre este tipo de tráfico y además indicarles a los usuarios con direcciones IP repetidas en el análisis de TOR, que el uso de software para saltar las restricciones de Internet puede llegar a poner en riesgo la seguridad de la información.

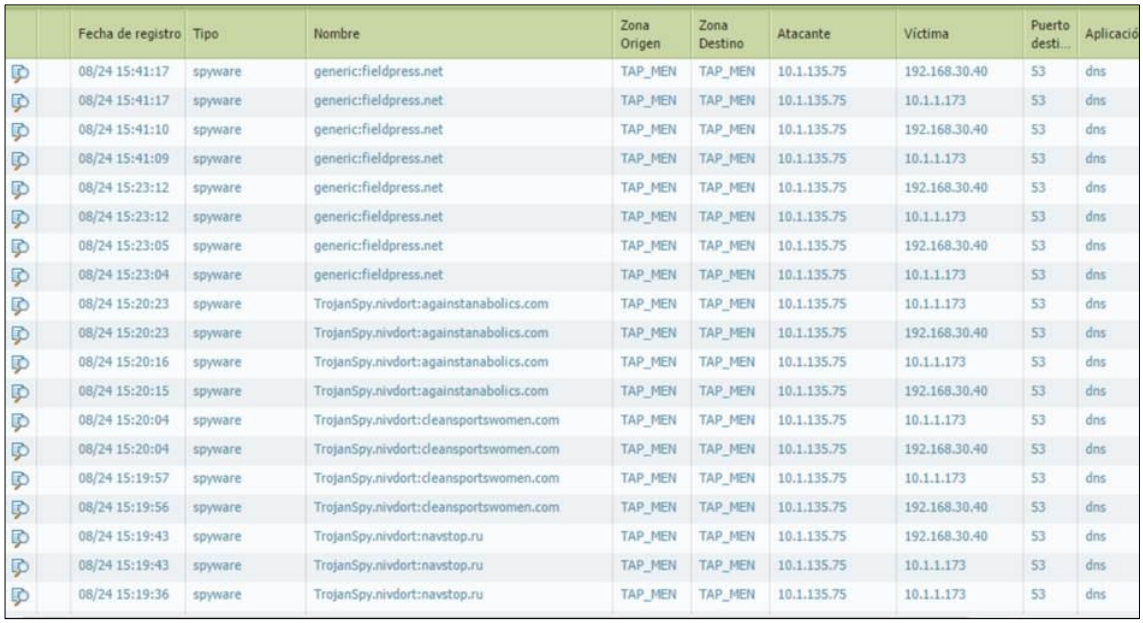
- **Detección de amenaza miércoles 24/8/2016**

Solicito por favor se lleve a cabo la instalación del paquete antivirus y análisis sobre el *endpoint* con IP 10.1.120.146 con *hostname* anmoralesa, ya que producto del análisis de logs de los NGFW Palo Alto se evidencio que está generando tráfico tipo "*spyware*" y se tienen altos indicios de estar infectado, como se observa en la figura 13,14:

Figura 13. Detección de amenaza estadística - miércoles 24/8/2016

Fuente: *Dashboard* del NGFW CAN.

Figura 14. Detección de amenaza - miércoles 24/8/2016

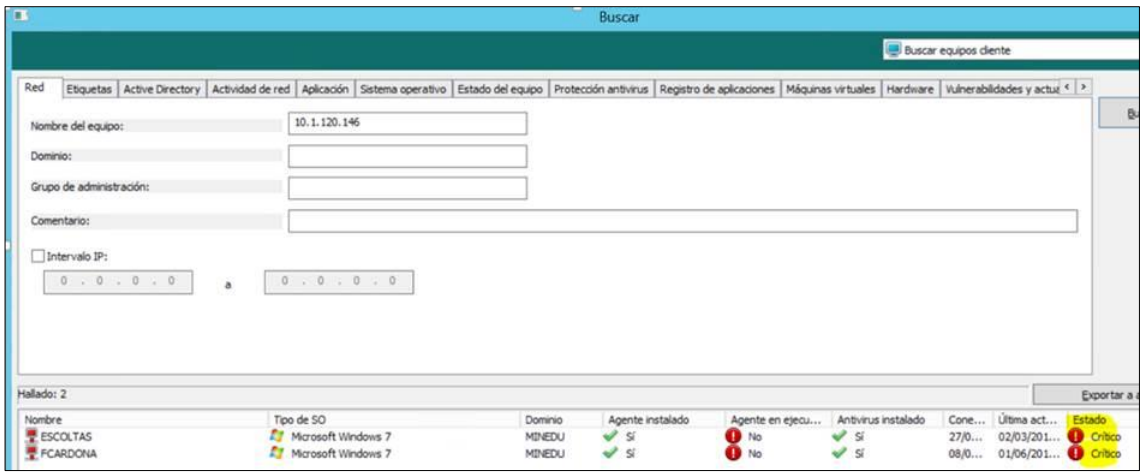


	Fecha de registro	Tipo	Nombre	Zona Origen	Zona Destino	Atacante	Víctima	Puerto desti...	Aplicació
	08/24 15:41:17	spyware	generic:fieldpress.net	TAP_MEN	TAP_MEN	10.1.135.75	192.168.30.40	53	dns
	08/24 15:41:17	spyware	generic:fieldpress.net	TAP_MEN	TAP_MEN	10.1.135.75	10.1.1.173	53	dns
	08/24 15:41:10	spyware	generic:fieldpress.net	TAP_MEN	TAP_MEN	10.1.135.75	192.168.30.40	53	dns
	08/24 15:41:09	spyware	generic:fieldpress.net	TAP_MEN	TAP_MEN	10.1.135.75	10.1.1.173	53	dns
	08/24 15:23:12	spyware	generic:fieldpress.net	TAP_MEN	TAP_MEN	10.1.135.75	192.168.30.40	53	dns
	08/24 15:23:12	spyware	generic:fieldpress.net	TAP_MEN	TAP_MEN	10.1.135.75	10.1.1.173	53	dns
	08/24 15:23:05	spyware	generic:fieldpress.net	TAP_MEN	TAP_MEN	10.1.135.75	192.168.30.40	53	dns
	08/24 15:23:04	spyware	generic:fieldpress.net	TAP_MEN	TAP_MEN	10.1.135.75	10.1.1.173	53	dns
	08/24 15:20:23	spyware	TrojanSpy.nivdort:againstanabolics.com	TAP_MEN	TAP_MEN	10.1.135.75	10.1.1.173	53	dns
	08/24 15:20:23	spyware	TrojanSpy.nivdort:againstanabolics.com	TAP_MEN	TAP_MEN	10.1.135.75	192.168.30.40	53	dns
	08/24 15:20:16	spyware	TrojanSpy.nivdort:againstanabolics.com	TAP_MEN	TAP_MEN	10.1.135.75	10.1.1.173	53	dns
	08/24 15:20:15	spyware	TrojanSpy.nivdort:againstanabolics.com	TAP_MEN	TAP_MEN	10.1.135.75	192.168.30.40	53	dns
	08/24 15:20:04	spyware	TrojanSpy.nivdort:cleansportswomen.com	TAP_MEN	TAP_MEN	10.1.135.75	10.1.1.173	53	dns
	08/24 15:20:04	spyware	TrojanSpy.nivdort:cleansportswomen.com	TAP_MEN	TAP_MEN	10.1.135.75	192.168.30.40	53	dns
	08/24 15:19:57	spyware	TrojanSpy.nivdort:cleansportswomen.com	TAP_MEN	TAP_MEN	10.1.135.75	10.1.1.173	53	dns
	08/24 15:19:56	spyware	TrojanSpy.nivdort:cleansportswomen.com	TAP_MEN	TAP_MEN	10.1.135.75	192.168.30.40	53	dns
	08/24 15:19:43	spyware	TrojanSpy.nivdort:navstop.ru	TAP_MEN	TAP_MEN	10.1.135.75	192.168.30.40	53	dns
	08/24 15:19:43	spyware	TrojanSpy.nivdort:navstop.ru	TAP_MEN	TAP_MEN	10.1.135.75	10.1.1.173	53	dns
	08/24 15:19:36	spyware	TrojanSpy.nivdort:navstop.ru	TAP_MEN	TAP_MEN	10.1.135.75	10.1.1.173	53	dns

Fuente: Logs NGFW CAN.

En la figura 15 se observa que la IP 10.1.12.146 corresponde al pc de escoltas el cual no cuenta con antivirus instalado y el estado es crítico:

Figura 15. Validación de antivirus en el *endpoint* respecto a la amenaza del NGFW.

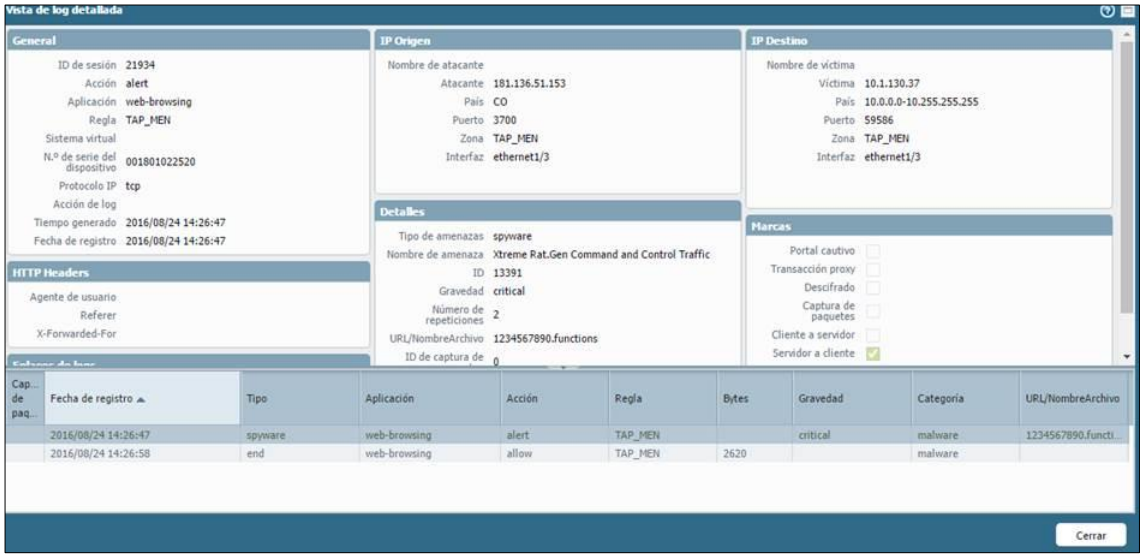


Fuente: Consola Antivirus Kaspersky.

- **Detección de amenaza miércoles 24/8/2016**

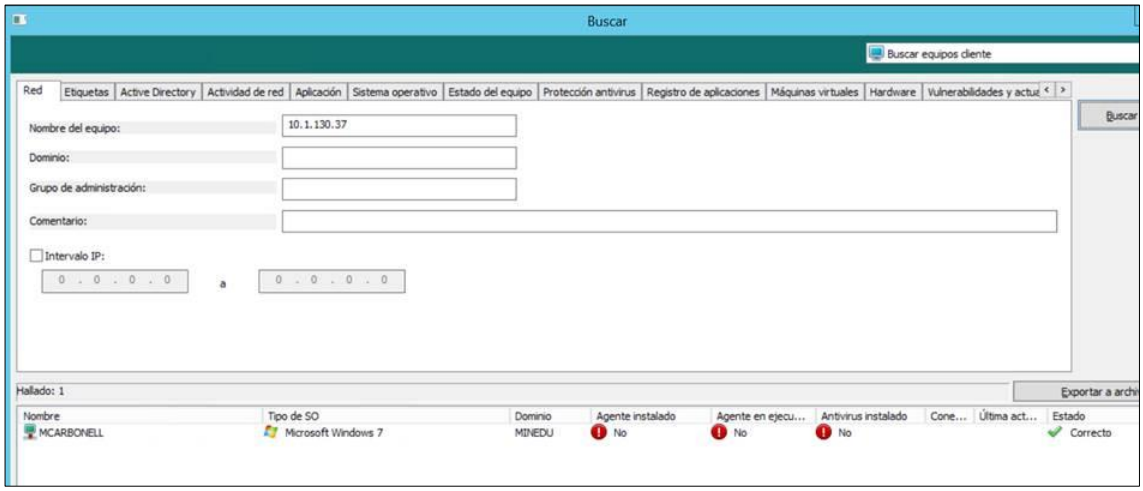
Solicito por favor se realice la instalación del paquete antivirus y análisis sobre el *endpoint* con IP 10.1.130.37 con *hostname* mcarbonell, ya que producto del análisis de logs de los NGFW Palo Alto se evidencio que está generando tráfico tipo "*malware*" y se tienen altos indicios de estar infectado como se observa en la figura 16, adicionalmente se observa que no tiene instalado en antivirus como se observa en la figura 17, a continuación, se observa las evidencias:

Figura 16. Detección de amenaza miércoles 24/8/2016



Fuente: Logs NGFW CAN.

Figura 17. Validación de antivirus en el *endpoint* respecto a la amenaza del NGFW

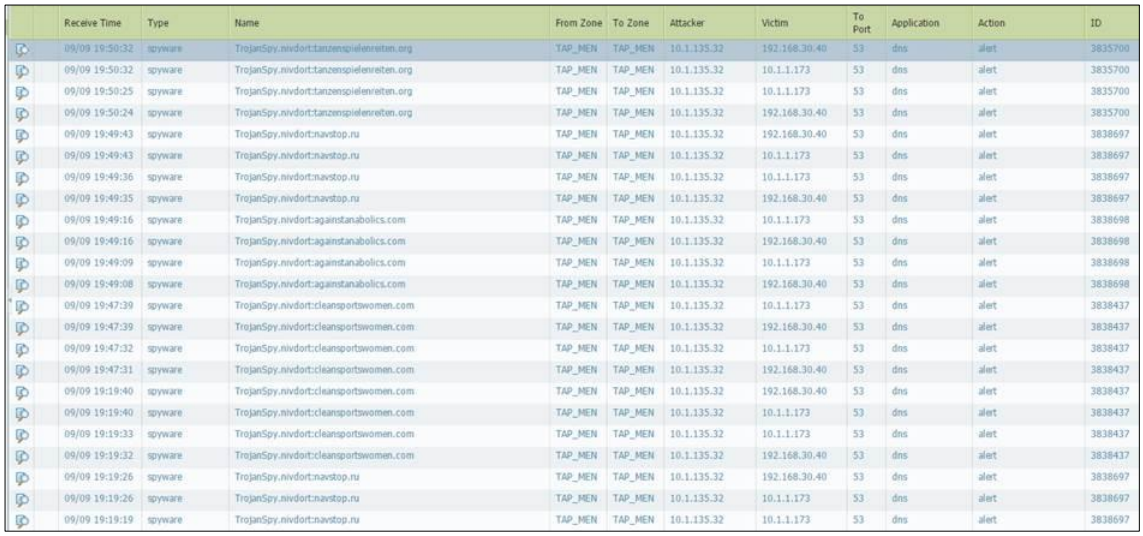


Fuente: Consola Antivirus Kaspersky

- **Detección de amenaza martes 13/9/2016**

Solicito por favor se realice la instalación del paquete antivirus y análisis sobre el *endpoint* con IP 10.1.135.32 con *hostname* camorales, ya que producto del análisis de logs de los NGFW Palo Alto se evidencio que está generando tráfico tipo "*spyware*" y se tienen altos indicios de estar infectado como se puede evidenciar en la figura 18, adicionalmente se observa como estado crítico en la consola antivirus como se observa en la figura 19:

Figura 18. Detección de amenaza martes 13/9/2016

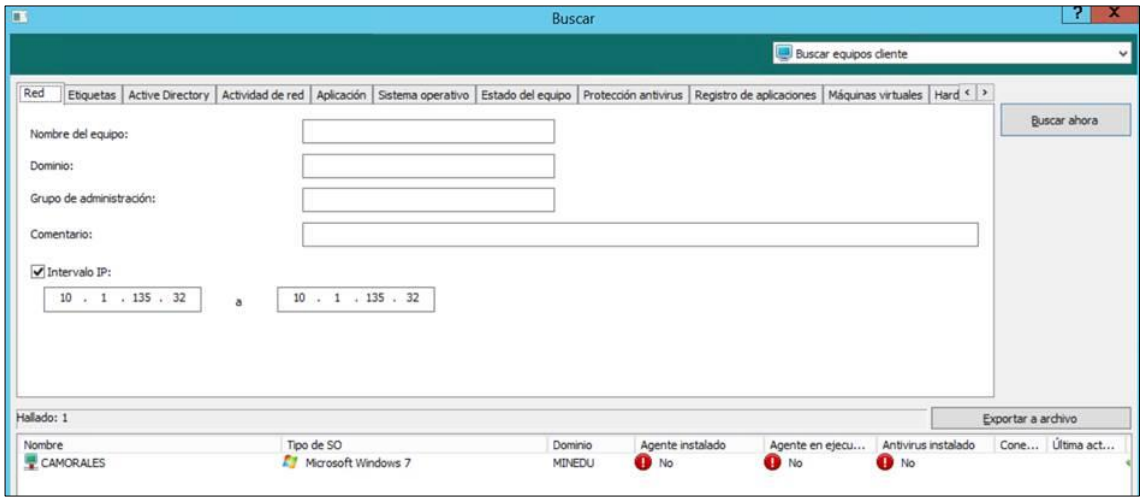


Receive Time	Type	Name	From Zone	To Zone	Attacker	Victim	To Port	Application	Action	ID
09/09 19:50:32	spyware	TrojanSpy.nivdort:tanzenspielenreiten.org	TAP_MEN	TAP_MEN	10.1.135.32	192.168.30.40	53	dns	alert	3835700
09/09 19:50:32	spyware	TrojanSpy.nivdort:tanzenspielenreiten.org	TAP_MEN	TAP_MEN	10.1.135.32	10.1.1.173	53	dns	alert	3835700
09/09 19:50:25	spyware	TrojanSpy.nivdort:tanzenspielenreiten.org	TAP_MEN	TAP_MEN	10.1.135.32	10.1.1.173	53	dns	alert	3835700
09/09 19:50:24	spyware	TrojanSpy.nivdort:tanzenspielenreiten.org	TAP_MEN	TAP_MEN	10.1.135.32	192.168.30.40	53	dns	alert	3835700
09/09 19:49:43	spyware	TrojanSpy.nivdort:navstop.ru	TAP_MEN	TAP_MEN	10.1.135.32	192.168.30.40	53	dns	alert	3838697
09/09 19:49:43	spyware	TrojanSpy.nivdort:navstop.ru	TAP_MEN	TAP_MEN	10.1.135.32	10.1.1.173	53	dns	alert	3838697
09/09 19:49:36	spyware	TrojanSpy.nivdort:navstop.ru	TAP_MEN	TAP_MEN	10.1.135.32	10.1.1.173	53	dns	alert	3838697
09/09 19:49:35	spyware	TrojanSpy.nivdort:navstop.ru	TAP_MEN	TAP_MEN	10.1.135.32	192.168.30.40	53	dns	alert	3838697
09/09 19:49:16	spyware	TrojanSpy.nivdort:againstanabolics.com	TAP_MEN	TAP_MEN	10.1.135.32	10.1.1.173	53	dns	alert	3838698
09/09 19:49:16	spyware	TrojanSpy.nivdort:againstanabolics.com	TAP_MEN	TAP_MEN	10.1.135.32	192.168.30.40	53	dns	alert	3838698
09/09 19:49:09	spyware	TrojanSpy.nivdort:againstanabolics.com	TAP_MEN	TAP_MEN	10.1.135.32	10.1.1.173	53	dns	alert	3838698
09/09 19:49:08	spyware	TrojanSpy.nivdort:againstanabolics.com	TAP_MEN	TAP_MEN	10.1.135.32	192.168.30.40	53	dns	alert	3838698
09/09 19:47:39	spyware	TrojanSpy.nivdort:cleansportswomen.com	TAP_MEN	TAP_MEN	10.1.135.32	10.1.1.173	53	dns	alert	3838437
09/09 19:47:39	spyware	TrojanSpy.nivdort:cleansportswomen.com	TAP_MEN	TAP_MEN	10.1.135.32	192.168.30.40	53	dns	alert	3838437
09/09 19:47:32	spyware	TrojanSpy.nivdort:cleansportswomen.com	TAP_MEN	TAP_MEN	10.1.135.32	10.1.1.173	53	dns	alert	3838437
09/09 19:47:31	spyware	TrojanSpy.nivdort:cleansportswomen.com	TAP_MEN	TAP_MEN	10.1.135.32	192.168.30.40	53	dns	alert	3838437
09/09 19:19:40	spyware	TrojanSpy.nivdort:cleansportswomen.com	TAP_MEN	TAP_MEN	10.1.135.32	192.168.30.40	53	dns	alert	3838437
09/09 19:19:40	spyware	TrojanSpy.nivdort:cleansportswomen.com	TAP_MEN	TAP_MEN	10.1.135.32	10.1.1.173	53	dns	alert	3838437
09/09 19:19:33	spyware	TrojanSpy.nivdort:cleansportswomen.com	TAP_MEN	TAP_MEN	10.1.135.32	10.1.1.173	53	dns	alert	3838437
09/09 19:19:32	spyware	TrojanSpy.nivdort:cleansportswomen.com	TAP_MEN	TAP_MEN	10.1.135.32	192.168.30.40	53	dns	alert	3838437
09/09 19:19:26	spyware	TrojanSpy.nivdort:navstop.ru	TAP_MEN	TAP_MEN	10.1.135.32	192.168.30.40	53	dns	alert	3838697
09/09 19:19:26	spyware	TrojanSpy.nivdort:navstop.ru	TAP_MEN	TAP_MEN	10.1.135.32	10.1.1.173	53	dns	alert	3838697
09/09 19:19:19	spyware	TrojanSpy.nivdort:navstop.ru	TAP_MEN	TAP_MEN	10.1.135.32	10.1.1.173	53	dns	alert	3838697

Fuente: Logs NGFW CAN.

De la consola Antivirus Kaspersky: Sobre el pc camorales no se encuentra dentro de la lista, es importante identificarlo y realizar la instalación del antivirus Kaspersky.

Figura 19. Validación de antivirus en el *endpoint* respecto a la amenaza del NGFW



Fuente: Consola antivirus Kaspersky.

- **Detección de amenaza jueves 22/9/2016**

Solicito por favor se realice la revisión si tienen instalado el paquete antivirus sobre los siguientes *endpoints*:

pruebasx-465acc
matorres_1
wisantamaria

De tener instalado el paquete antivirus por favor realizar actualización de la base de datos y lanzar un escaneo total, ya que producto del análisis de logs de los NGFW Palo Alto, se evidenció que se está generando tráfico tipo "*spyware*" y se tienen altos indicios de estar infectados como se evidencia en la figura 20, 21 y 22 para cada uno de los *endpoints*.

Para la IP 10.1.110.134 con nombre equipo pruebasx-465acc:

Figura 20. Detección de amenaza - jueves 22/9/2016

	Receive Time	Type	Name	From Zone	To Zone	Attacker	Victim	To Port	Application	Action	ID	Severity
	09/22 09:07:56	spyware	Suspicious DNS Query (generic:aqxqfyyfrb.net)	TAP_MEN	TAP_MEN	10.1.110.134	192.168.30.40	53	dns	alert	4072908	medium
	09/22 09:07:56	spyware	Suspicious DNS Query (generic:cewpnra.biz)	TAP_MEN	TAP_MEN	10.1.110.134	192.168.30.40	53	dns	alert	4072982	medium
	09/22 09:07:56	spyware	Suspicious DNS Query (generic:nzuaevn.cc)	TAP_MEN	TAP_MEN	10.1.110.134	192.168.30.40	53	dns	alert	4072861	medium
	09/22 09:07:56	spyware	Suspicious DNS Query (generic:pjahwpud.net)	TAP_MEN	TAP_MEN	10.1.110.134	192.168.30.40	53	dns	alert	4072896	medium
	09/22 09:07:56	spyware	Suspicious DNS Query (generic:fdpughfi.org)	TAP_MEN	TAP_MEN	10.1.110.134	192.168.30.40	53	dns	alert	4072918	medium
	09/22 09:07:56	spyware	Suspicious DNS Query (generic:daqjpoahht.net)	TAP_MEN	TAP_MEN	10.1.110.134	192.168.30.40	53	dns	alert	4072900	medium
	09/22 09:07:56	spyware	Suspicious DNS Query (generic:ttpgurwo.cn)	TAP_MEN	TAP_MEN	10.1.110.134	192.168.30.40	53	dns	alert	4058180	medium
	09/22 09:07:52	spyware	Suspicious DNS Query (generic:cewpnra.biz)	TAP_MEN	TAP_MEN	10.1.110.134	10.1.1.173	53	dns	alert	4072982	medium
	09/22 09:07:52	spyware	Suspicious DNS Query (generic:aqxqfyyfrb.net)	TAP_MEN	TAP_MEN	10.1.110.134	10.1.1.173	53	dns	alert	4072908	medium
	09/22 09:07:52	spyware	Suspicious DNS Query (generic:nzuaevn.cc)	TAP_MEN	TAP_MEN	10.1.110.134	10.1.1.173	53	dns	alert	4072861	medium
	09/22 09:07:52	spyware	Suspicious DNS Query (generic:pjahwpud.net)	TAP_MEN	TAP_MEN	10.1.110.134	10.1.1.173	53	dns	alert	4072896	medium
	09/22 09:07:52	spyware	Suspicious DNS Query (generic:fdpughfi.org)	TAP_MEN	TAP_MEN	10.1.110.134	10.1.1.173	53	dns	alert	4072918	medium
	09/22 09:07:52	spyware	Suspicious DNS Query (generic:ttpgurwo.cn)	TAP_MEN	TAP_MEN	10.1.110.134	10.1.1.173	53	dns	alert	4058180	medium
	09/22 09:07:52	spyware	Suspicious DNS Query (generic:daqjpoahht.net)	TAP_MEN	TAP_MEN	10.1.110.134	10.1.1.173	53	dns	alert	4072900	medium
	09/22 09:07:48	spyware	Suspicious DNS Query (generic:aqxqfyyfrb.net)	TAP_MEN	TAP_MEN	10.1.110.134	192.168.30.40	53	dns	alert	4072908	medium
	09/22 09:07:48	spyware	Suspicious DNS Query (generic:cewpnra.biz)	TAP_MEN	TAP_MEN	10.1.110.134	192.168.30.40	53	dns	alert	4072982	medium
	09/22 09:07:48	spyware	Suspicious DNS Query (generic:nzuaevn.cc)	TAP_MEN	TAP_MEN	10.1.110.134	192.168.30.40	53	dns	alert	4072861	medium
	09/22 09:07:48	spyware	Suspicious DNS Query (generic:ttpgurwo.cn)	TAP_MEN	TAP_MEN	10.1.110.134	192.168.30.40	53	dns	alert	4058180	medium
	09/22 09:07:48	spyware	Suspicious DNS Query (generic:pjahwpud.net)	TAP_MEN	TAP_MEN	10.1.110.134	192.168.30.40	53	dns	alert	4072896	medium
	09/22 09:07:48	spyware	Suspicious DNS Query (generic:fdpughfi.org)	TAP_MEN	TAP_MEN	10.1.110.134	192.168.30.40	53	dns	alert	4072918	medium
	09/22 09:07:48	spyware	Suspicious DNS Query (generic:daqjpoahht.net)	TAP_MEN	TAP_MEN	10.1.110.134	192.168.30.40	53	dns	alert	4072900	medium
	09/22 09:07:33	spyware	Suspicious DNS Query (generic:trgcrbdhe.org)	TAP_MEN	TAP_MEN	10.1.110.134	192.168.30.40	53	dns	alert	4072774	medium
	09/22 09:07:33	spyware	Suspicious DNS Query (generic:rndkytj.cc)	TAP_MEN	TAP_MEN	10.1.110.134	192.168.30.40	53	dns	alert	4072944	medium
	09/22 09:07:33	spyware	Suspicious DNS Query (generic:trdxeqp.info)	TAP_MEN	TAP_MEN	10.1.110.134	192.168.30.40	53	dns	alert	4072777	medium
	09/22 09:07:33	spyware	Suspicious DNS Query (generic:mkkof.org)	TAP_MEN	TAP_MEN	10.1.110.134	192.168.30.40	53	dns	alert	4073215	medium

Fuente: Logs NGFW CAN.

Para la IP 10.1.145.96 con nombre de equipo matorres_1:

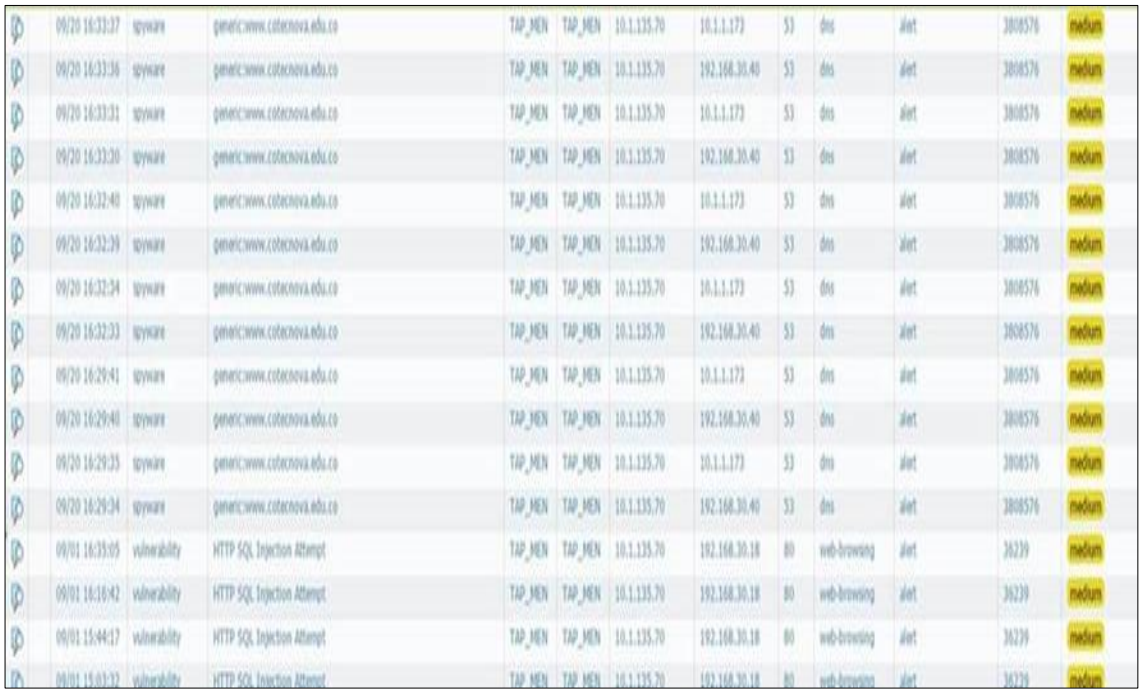
Figura 21. Detección de amenaza - jueves 22/9/2016

Receive Time	Type	Name	From Zone	To Zone	Attacker	Victim	To Port	Application	Action	ID	Severity
09/22 07:18:34	spyware	PWS.vb:popkeyservice.bd-pl.com	TAP_MEN	TAP_MEN	10.1.145.96	10.1.1.173	53	dns	alert	3826736	medium
09/22 07:18:33	spyware	PWS.vb:popkeyservice.bd-pl.com	TAP_MEN	TAP_MEN	10.1.145.96	192.168.30.40	53	dns	alert	3826736	medium
09/22 07:18:28	spyware	PWS.vb:popkeyservice.bd-pl.com	TAP_MEN	TAP_MEN	10.1.145.96	10.1.1.173	53	dns	alert	3826736	medium
09/22 07:18:27	spyware	PWS.vb:popkeyservice.bd-pl.com	TAP_MEN	TAP_MEN	10.1.145.96	192.168.30.40	53	dns	alert	3826736	medium
09/22 07:17:34	vulnerability	Microsoft Windows SMB Negotiate Request	TAP_MEN	TAP_MEN	10.1.145.96	10.1.1.137	445	ms-ds-smb	alert	35364	informational
09/21 17:58:57	spyware	PWS.vb:popkeyservice.bd-pl.com	TAP_MEN	TAP_MEN	10.1.145.96	10.1.1.173	53	dns	alert	3826736	medium
09/21 17:58:57	spyware	PWS.vb:popkeyservice.bd-pl.com	TAP_MEN	TAP_MEN	10.1.145.96	192.168.30.40	53	dns	alert	3826736	medium
09/21 17:58:50	spyware	PWS.vb:popkeyservice.bd-pl.com	TAP_MEN	TAP_MEN	10.1.145.96	10.1.1.173	53	dns	alert	3826736	medium
09/21 17:58:49	spyware	PWS.vb:popkeyservice.bd-pl.com	TAP_MEN	TAP_MEN	10.1.145.96	192.168.30.40	53	dns	alert	3826736	medium
09/21 16:07:28	vulnerability	Microsoft Windows SMB Negotiate Request	TAP_MEN	TAP_MEN	10.1.145.96	10.1.1.137	445	ms-ds-smb	alert	35364	informational
09/21 14:26:25	spyware	PWS.vb:popkeyservice.bd-pl.com	TAP_MEN	TAP_MEN	10.1.145.96	10.1.1.173	53	dns	alert	3826736	medium
09/21 14:26:24	spyware	PWS.vb:popkeyservice.bd-pl.com	TAP_MEN	TAP_MEN	10.1.145.96	192.168.30.40	53	dns	alert	3826736	medium
09/21 14:26:19	spyware	PWS.vb:popkeyservice.bd-pl.com	TAP_MEN	TAP_MEN	10.1.145.96	10.1.1.173	53	dns	alert	3826736	medium
09/21 14:26:18	spyware	PWS.vb:popkeyservice.bd-pl.com	TAP_MEN	TAP_MEN	10.1.145.96	192.168.30.40	53	dns	alert	3826736	medium
09/21 14:25:32	vulnerability	Microsoft Windows SMB Negotiate Request	TAP_MEN	TAP_MEN	10.1.145.96	10.1.1.137	445	ms-ds-smb	alert	35364	informational
09/21 12:11:12	vulnerability	Microsoft Windows SMB Negotiate Request	TAP_MEN	TAP_MEN	10.1.145.96	10.1.1.137	445	ms-ds-smb	alert	35364	informational
09/21 11:20:46	vulnerability	Microsoft Windows SMB Negotiate Request	TAP_MEN	TAP_MEN	10.1.145.96	10.1.1.137	445	ms-ds-smb	alert	35364	informational
09/21 10:18:14	vulnerability	Microsoft Windows SMB Negotiate Request	TAP_MEN	TAP_MEN	10.1.145.96	10.1.1.137	445	ms-ds-smb	alert	35364	informational
09/21 08:29:30	spyware	PWS.vb:popkeyservice.bd-pl.com	TAP_MEN	TAP_MEN	10.1.145.96	10.1.1.173	53	dns	alert	3826736	medium
09/21 08:29:29	spyware	PWS.vb:popkeyservice.bd-pl.com	TAP_MEN	TAP_MEN	10.1.145.96	192.168.30.40	53	dns	alert	3826736	medium
09/21 08:29:24	spyware	PWS.vb:popkeyservice.bd-pl.com	TAP_MEN	TAP_MEN	10.1.145.96	10.1.1.173	53	dns	alert	3826736	medium
09/21 08:29:23	spyware	PWS.vb:popkeyservice.bd-pl.com	TAP_MEN	TAP_MEN	10.1.145.96	192.168.30.40	53	dns	alert	3826736	medium

Fuente: Logs NGFW CAN.

Para la IP 10.1.135.70 con nombre de equipo wisantamaria:

Figura 22. Detección de amenaza - jueves 22/9/2016



09/20 16:33:27	spyware	generic:www.cotecnova.edu.co	TAP_MEN	TAP_MEN	10.1.135.70	10.1.1.173	53	dns	alert	3808576	medium
09/20 16:33:36	spyware	generic:www.cotecnova.edu.co	TAP_MEN	TAP_MEN	10.1.135.70	192.168.30.40	53	dns	alert	3808576	medium
09/20 16:33:31	spyware	generic:www.cotecnova.edu.co	TAP_MEN	TAP_MEN	10.1.135.70	10.1.1.173	53	dns	alert	3808576	medium
09/20 16:33:20	spyware	generic:www.cotecnova.edu.co	TAP_MEN	TAP_MEN	10.1.135.70	192.168.30.40	53	dns	alert	3808576	medium
09/20 16:32:40	spyware	generic:www.cotecnova.edu.co	TAP_MEN	TAP_MEN	10.1.135.70	10.1.1.173	53	dns	alert	3808576	medium
09/20 16:32:29	spyware	generic:www.cotecnova.edu.co	TAP_MEN	TAP_MEN	10.1.135.70	192.168.30.40	53	dns	alert	3808576	medium
09/20 16:32:24	spyware	generic:www.cotecnova.edu.co	TAP_MEN	TAP_MEN	10.1.135.70	10.1.1.173	53	dns	alert	3808576	medium
09/20 16:32:23	spyware	generic:www.cotecnova.edu.co	TAP_MEN	TAP_MEN	10.1.135.70	192.168.30.40	53	dns	alert	3808576	medium
09/20 16:29:41	spyware	generic:www.cotecnova.edu.co	TAP_MEN	TAP_MEN	10.1.135.70	10.1.1.173	53	dns	alert	3808576	medium
09/20 16:29:40	spyware	generic:www.cotecnova.edu.co	TAP_MEN	TAP_MEN	10.1.135.70	192.168.30.40	53	dns	alert	3808576	medium
09/20 16:29:25	spyware	generic:www.cotecnova.edu.co	TAP_MEN	TAP_MEN	10.1.135.70	10.1.1.173	53	dns	alert	3808576	medium
09/20 16:29:24	spyware	generic:www.cotecnova.edu.co	TAP_MEN	TAP_MEN	10.1.135.70	192.168.30.40	53	dns	alert	3808576	medium
09/01 16:35:05	vulnerability	HTTP SQL Injection Attempt	TAP_MEN	TAP_MEN	10.1.135.70	192.168.30.18	80	web-browsing	alert	36239	medium
09/01 16:16:42	vulnerability	HTTP SQL Injection Attempt	TAP_MEN	TAP_MEN	10.1.135.70	192.168.30.18	80	web-browsing	alert	36239	medium
09/01 15:44:17	vulnerability	HTTP SQL Injection Attempt	TAP_MEN	TAP_MEN	10.1.135.70	192.168.30.18	80	web-browsing	alert	36239	medium
09/01 15:03:22	vulnerability	HTTP SQL Injection Attempt	TAP_MEN	TAP_MEN	10.1.135.70	192.168.30.18	80	web-browsing	alert	36239	medium

Fuente: Logs NGFW CAN.

- **Detección de amenaza jueves 6/10/2016**

Solicito por favor se realice la revisión si tienen instalado el paquete antivirus sobre el *endpoints* de azambrano1, si tiene instalado el paquete antivirus por favor realizar actualización de la base de datos y lanzar un escaneo total, ya que producto del análisis de logs de los NGFW Palo Alto, se evidenció que se está generando tráfico tipo "*spyware*" y se tienen altos indicios de estar infectados como se evidencia en la figura 23.

Para la IP 10.1.130.58 con nombre equipo azambrano1:

Figura 23. Detección de amenaza - jueves 6/10/2016

Receive Time	Type	Name	From Zone	To Zone	Attacker	Victim	To Port	Application	Action	ID	Severity
10/06 08:56:35	spyware	Suspicious DNS Query (generic:duckdns4.duckdns.org)	TAP_MEN	TAP_MEN	10.1.130.58	192.168.30.40	53	dns	alert	4015907	medium
10/06 08:56:31	spyware	Suspicious DNS Query (generic:duckdns4.duckdns.org)	TAP_MEN	TAP_MEN	10.1.130.58	10.1.1.173	53	dns	alert	4015907	medium
10/06 08:56:27	spyware	Suspicious DNS Query (generic:duckdns4.duckdns.org)	TAP_MEN	TAP_MEN	10.1.130.58	192.168.30.40	53	dns	alert	4015907	medium
10/06 08:56:18	spyware	Suspicious DNS Query (generic:duckdns4.duckdns.org)	TAP_MEN	TAP_MEN	10.1.130.58	192.168.30.40	53	dns	alert	4015907	medium
10/06 08:56:12	spyware	Suspicious DNS Query (generic:duckdns4.duckdns.org)	TAP_MEN	TAP_MEN	10.1.130.58	192.168.30.40	53	dns	alert	4015907	medium
10/06 08:56:10	spyware	Suspicious DNS Query (generic:duckdns4.duckdns.org)	TAP_MEN	TAP_MEN	10.1.130.58	10.1.1.173	53	dns	alert	4015907	medium
10/06 08:56:01	spyware	Suspicious DNS Query (generic:duckdns4.duckdns.org)	TAP_MEN	TAP_MEN	10.1.130.58	192.168.30.40	53	dns	alert	4015907	medium
10/06 08:55:57	spyware	Suspicious DNS Query (generic:duckdns4.duckdns.org)	TAP_MEN	TAP_MEN	10.1.130.58	10.1.1.173	53	dns	alert	4015907	medium
10/06 08:55:53	spyware	Suspicious DNS Query (generic:duckdns4.duckdns.org)	TAP_MEN	TAP_MEN	10.1.130.58	192.168.30.40	53	dns	alert	4015907	medium
10/06 08:55:44	spyware	Suspicious DNS Query (generic:duckdns4.duckdns.org)	TAP_MEN	TAP_MEN	10.1.130.58	10.1.1.173	53	dns	alert	4015907	medium
10/06 08:55:44	spyware	Suspicious DNS Query (generic:duckdns4.duckdns.org)	TAP_MEN	TAP_MEN	10.1.130.58	192.168.30.40	53	dns	alert	4015907	medium
10/06 08:55:38	spyware	Suspicious DNS Query (generic:duckdns4.duckdns.org)	TAP_MEN	TAP_MEN	10.1.130.58	192.168.30.40	53	dns	alert	4015907	medium
10/06 08:55:36	spyware	Suspicious DNS Query (generic:duckdns4.duckdns.org)	TAP_MEN	TAP_MEN	10.1.130.58	10.1.1.173	53	dns	alert	4015907	medium
10/06 08:55:27	spyware	Suspicious DNS Query (generic:duckdns4.duckdns.org)	TAP_MEN	TAP_MEN	10.1.130.58	192.168.30.40	53	dns	alert	4015907	medium
10/06 08:55:23	spyware	Suspicious DNS Query (generic:duckdns4.duckdns.org)	TAP_MEN	TAP_MEN	10.1.130.58	10.1.1.173	53	dns	alert	4015907	medium
10/06 08:55:19	spyware	Suspicious DNS Query (generic:duckdns4.duckdns.org)	TAP_MEN	TAP_MEN	10.1.130.58	192.168.30.40	53	dns	alert	4015907	medium
10/06 08:55:10	spyware	Suspicious DNS Query (generic:duckdns4.duckdns.org)	TAP_MEN	TAP_MEN	10.1.130.58	10.1.1.173	53	dns	alert	4015907	medium
10/06 08:55:10	spyware	Suspicious DNS Query (generic:duckdns4.duckdns.org)	TAP_MEN	TAP_MEN	10.1.130.58	192.168.30.40	53	dns	alert	4015907	medium
10/06 08:55:04	spyware	Suspicious DNS Query (generic:duckdns4.duckdns.org)	TAP_MEN	TAP_MEN	10.1.130.58	192.168.30.40	53	dns	alert	4015907	medium
10/06 08:55:02	spyware	Suspicious DNS Query (generic:duckdns4.duckdns.org)	TAP_MEN	TAP_MEN	10.1.130.58	10.1.1.173	53	dns	alert	4015907	medium
10/06 08:54:53	spyware	Suspicious DNS Query (generic:duckdns4.duckdns.org)	TAP_MEN	TAP_MEN	10.1.130.58	192.168.30.40	53	dns	alert	4015907	medium
10/06 08:54:49	spyware	Suspicious DNS Query (generic:duckdns4.duckdns.org)	TAP_MEN	TAP_MEN	10.1.130.58	10.1.1.173	53	dns	alert	4015907	medium
10/06 08:54:45	spyware	Suspicious DNS Query (generic:duckdns4.duckdns.org)	TAP_MEN	TAP_MEN	10.1.130.58	192.168.30.40	53	dns	alert	4015907	medium
10/06 08:54:36	spyware	Suspicious DNS Query (generic:duckdns4.duckdns.org)	TAP_MEN	TAP_MEN	10.1.130.58	192.168.30.40	53	dns	alert	4015907	medium
10/06 08:54:32	spyware	Suspicious DNS Query (generic:duckdns4.duckdns.org)	TAP_MEN	TAP_MEN	10.1.130.58	10.1.1.173	53	dns	alert	4015907	medium

Fuente: Logs NGFW CAN.

- **Detección de amenaza - miércoles 12/10/2016**

Solicito por favor se valide si tienen instalado el paquete antivirus sobre el *endpoint* de mruiz1 con direccionamiento 10.1.4.163 perteneciente a la red de WIFI, si tiene instalado el paquete antivirus por favor realizar actualización de la base de datos y lanzar un escaneo total adicionalmente se sugiere validar directamente en la máquina del usuario para evidenciar que no tenga instalado ninguna herramienta sospechosa, de ser necesario se sugiere bloquear su conexión por la WIFI, ya que producto del análisis de logs de los NGFW Palo Alto, se evidenció que está activando firmas de amenaza tipo (*médium y high*) como se evidencia en la figura 24.

Figura 24. Detección de amenaza - miércoles 12/10/2016

Receive Time	Type	Name	From Zone	To Zone	Attacker	Victim	To Port	Application	Action	ID	Severity
10/12 15:27:33	vulnerability	HTTP SQL Injection Attempt	TAP_MEN	TAP_MEN	10.1.4.163	192.168.30.18	80	web-browsing	alert	36239	medium
10/12 14:07:30	vulnerability	SMB: User Password Brute Force Attempt	TAP_DMZ	TAP_DMZ	10.1.4.163	192.168.30.67	445	ms-ds-smb	alert	40004	high
10/12 14:07:18	vulnerability	SMB: User Password Brute Force Attempt	TAP_DMZ	TAP_DMZ	10.1.4.163	192.168.30.67	445	ms-ds-smb	alert	40004	high
10/12 14:07:08	vulnerability	SMB: User Password Brute Force Attempt	TAP_MEN	TAP_MEN	10.1.4.163	192.168.30.67	445	ms-ds-smb	alert	40004	high
10/12 14:06:30	vulnerability	SMB: User Password Brute Force Attempt	TAP_DMZ	TAP_DMZ	10.1.4.163	192.168.30.67	445	ms-ds-smb	alert	40004	high
10/12 14:06:16	vulnerability	SMB: User Password Brute Force Attempt	TAP_DMZ	TAP_DMZ	10.1.4.163	192.168.30.67	445	ms-ds-smb	alert	40004	high
10/12 14:06:06	vulnerability	SMB: User Password Brute Force Attempt	TAP_MEN	TAP_MEN	10.1.4.163	192.168.30.67	445	ms-ds-smb	alert	40004	high
10/12 13:31:14	vulnerability	HTTP SQL Injection Attempt	TAP_MEN	TAP_MEN	10.1.4.163	192.168.30.18	80	web-browsing	alert	36239	medium
10/12 10:49:17	vulnerability	HTTP SQL Injection Attempt	TAP_MEN	TAP_MEN	10.1.4.163	192.168.30.18	80	web-browsing	alert	36239	medium
10/12 10:06:17	vulnerability	HTTP SQL Injection Attempt	TAP_MEN	TAP_MEN	10.1.4.163	192.168.30.18	80	web-browsing	alert	36239	medium
10/12 09:44:45	vulnerability	HTTP SQL Injection Attempt	TAP_MEN	TAP_MEN	10.1.4.163	192.168.30.18	80	web-browsing	alert	36239	medium
10/12 09:34:42	vulnerability	HTTP SQL Injection Attempt	TAP_MEN	TAP_MEN	10.1.4.163	192.168.30.18	80	web-browsing	alert	36239	medium
10/12 09:27:05	vulnerability	HTTP SQL Injection Attempt	TAP_MEN	TAP_MEN	10.1.4.163	192.168.30.18	80	web-browsing	alert	36239	medium
10/11 18:12:50	vulnerability	HTTP SQL Injection Attempt	TAP_MEN	TAP_MEN	10.1.4.163	192.168.30.18	80	web-browsing	alert	36239	medium
10/11 16:49:24	vulnerability	SMB: User Password Brute Force Attempt	TAP_DMZ	TAP_DMZ	10.1.4.163	192.168.30.67	445	ms-ds-smb	alert	40004	high
10/11 16:48:55	vulnerability	SMB: User Password Brute Force Attempt	TAP_MEN	TAP_MEN	10.1.4.163	192.168.30.67	445	ms-ds-smb	alert	40004	high
10/11 16:25:18	vulnerability	SMB: User Password Brute Force Attempt	TAP_MEN	TAP_MEN	10.1.4.163	192.168.30.67	445	ms-ds-smb	alert	40004	high
10/11 15:53:35	vulnerability	SMB: User Password Brute Force Attempt	TAP_MEN	TAP_MEN	10.1.4.163	192.168.30.67	445	ms-ds-smb	alert	40004	high
10/11 15:29:46	vulnerability	HTTP SQL Injection Attempt	TAP_MEN	TAP_MEN	10.1.4.163	192.168.30.18	80	web-browsing	alert	36239	medium
10/11 14:08:26	vulnerability	HTTP SQL Injection Attempt	TAP_MEN	TAP_MEN	10.1.4.163	192.168.30.18	80	web-browsing	alert	36239	medium
10/11 13:39:50	vulnerability	HTTP SQL Injection Attempt	TAP_MEN	TAP_MEN	10.1.4.163	192.168.30.18	80	web-browsing	alert	36239	medium
10/11 13:31:44	vulnerability	HTTP SQL Injection Attempt	TAP_MEN	TAP_MEN	10.1.4.163	192.168.30.18	80	web-browsing	alert	36239	medium
10/11 12:13:24	vulnerability	SMB: User Password Brute Force Attempt	TAP_DMZ	TAP_DMZ	10.1.4.163	192.168.30.67	445	ms-ds-smb	alert	40004	high
10/11 12:13:16	vulnerability	SMB: User Password Brute Force Attempt	TAP_DMZ	TAP_DMZ	10.1.4.163	192.168.30.67	445	ms-ds-smb	alert	40004	high
10/11 12:13:06	vulnerability	SMB: User Password Brute Force Attempt	TAP_MEN	TAP_MEN	10.1.4.163	192.168.30.67	445	ms-ds-smb	alert	40004	high
10/11 12:09:50	vulnerability	SMB: User Password Brute Force Attempt	TAP_MEN	TAP_MEN	10.1.4.163	192.168.30.67	445	ms-ds-smb	alert	40004	high
10/11 08:34:19	vulnerability	HTTP SQL Injection Attempt	TAP_MEN	TAP_MEN	10.1.4.163	192.168.30.18	80	web-browsing	alert	36239	medium

Fuente: Logs NGFW CAN.

- **Detección de amenaza miércoles 12/10/2016**

Solicito por favor validar si en los *endpoints* de jacaballero y zriano se tiene instalado el paquete antivirus de estar instalado en antivirus por favor revisar si base de datos se encuentra actualizado y finalmente lanzar un escaneo total, ya que producto del análisis de logs de los NGFW Palo Alto, se evidenció que se está generando tráfico tipo "*spyware*" y se tienen altos indicios de estar infectados como se observa en la figura 25 y 26.

Para la IP 10.1.145.119 con nombre equipo jacaballero:

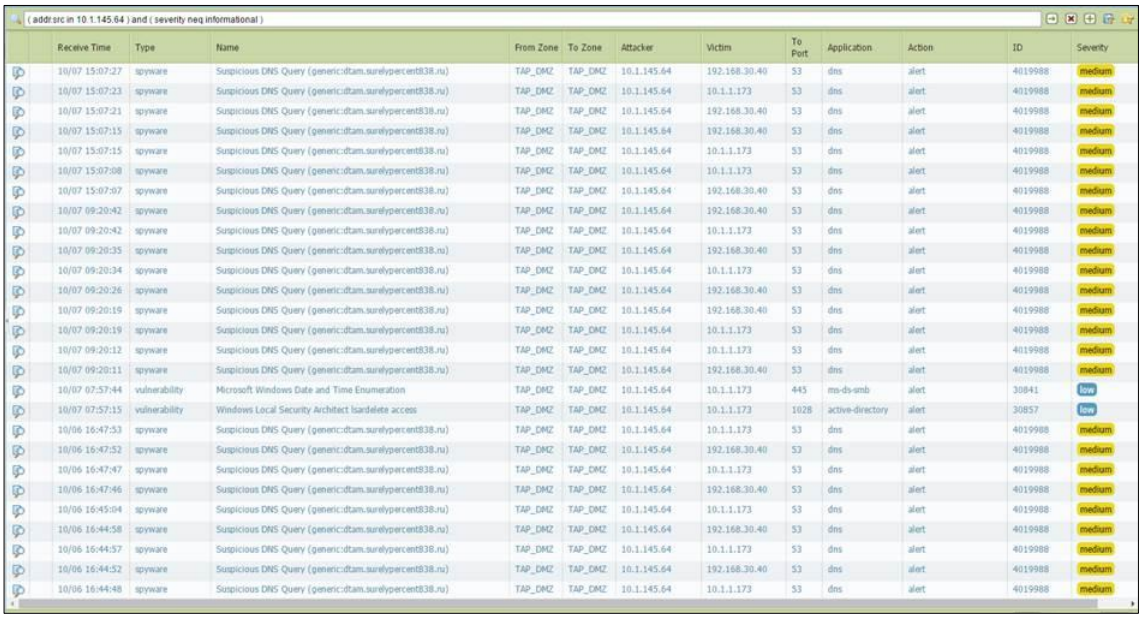
Figura 25. Detección de amenaza - miércoles 12/10/2016

Receive Time	Type	Name	From Zone	To Zone	Attacker	Victim	To Port	Application	Action	ID	Severity
10/07 10:41:23	spyware	Suspicious DNS Query (generic:dtam.surelypercent838.ru)	TAP_MEN	TAP_MEN	10.1.145.119	192.168.30.40	53	dns	alert	4019988	medium
10/07 10:41:19	spyware	Suspicious DNS Query (generic:dtam.surelypercent838.ru)	TAP_MEN	TAP_MEN	10.1.145.119	10.1.1.173	53	dns	alert	4019988	medium
10/07 10:41:17	spyware	Suspicious DNS Query (generic:dtam.surelypercent838.ru)	TAP_MEN	TAP_MEN	10.1.145.119	192.168.30.40	53	dns	alert	4019988	medium
10/07 10:41:13	spyware	Suspicious DNS Query (generic:dtam.surelypercent838.ru)	TAP_MEN	TAP_MEN	10.1.145.119	10.1.1.173	53	dns	alert	4019988	medium
10/07 10:40:48	spyware	Suspicious DNS Query (generic:dtam.surelypercent838.ru)	TAP_MEN	TAP_MEN	10.1.145.119	192.168.30.40	53	dns	alert	4019988	medium
10/07 10:40:44	spyware	Suspicious DNS Query (generic:dtam.surelypercent838.ru)	TAP_MEN	TAP_MEN	10.1.145.119	10.1.1.173	53	dns	alert	4019988	medium
10/07 10:40:42	spyware	Suspicious DNS Query (generic:dtam.surelypercent838.ru)	TAP_MEN	TAP_MEN	10.1.145.119	192.168.30.40	53	dns	alert	4019988	medium
10/07 10:40:38	spyware	Suspicious DNS Query (generic:dtam.surelypercent838.ru)	TAP_MEN	TAP_MEN	10.1.145.119	10.1.1.173	53	dns	alert	4019988	medium
10/07 10:40:12	spyware	Suspicious DNS Query (generic:dtam.surelypercent838.ru)	TAP_MEN	TAP_MEN	10.1.145.119	192.168.30.40	53	dns	alert	4019988	medium
10/07 10:40:08	spyware	Suspicious DNS Query (generic:dtam.surelypercent838.ru)	TAP_MEN	TAP_MEN	10.1.145.119	10.1.1.173	53	dns	alert	4019988	medium
10/07 10:40:06	spyware	Suspicious DNS Query (generic:dtam.surelypercent838.ru)	TAP_MEN	TAP_MEN	10.1.145.119	192.168.30.40	53	dns	alert	4019988	medium
10/07 10:40:02	spyware	Suspicious DNS Query (generic:dtam.surelypercent838.ru)	TAP_MEN	TAP_MEN	10.1.145.119	10.1.1.173	53	dns	alert	4019988	medium
10/07 10:39:54	spyware	Suspicious DNS Query (generic:dtam.surelypercent838.ru)	TAP_MEN	TAP_MEN	10.1.145.119	192.168.30.40	53	dns	alert	4019988	medium
10/07 10:39:50	spyware	Suspicious DNS Query (generic:dtam.surelypercent838.ru)	TAP_MEN	TAP_MEN	10.1.145.119	10.1.1.173	53	dns	alert	4019988	medium
10/07 10:39:48	spyware	Suspicious DNS Query (generic:dtam.surelypercent838.ru)	TAP_MEN	TAP_MEN	10.1.145.119	192.168.30.40	53	dns	alert	4019988	medium
10/07 10:39:44	spyware	Suspicious DNS Query (generic:dtam.surelypercent838.ru)	TAP_MEN	TAP_MEN	10.1.145.119	10.1.1.173	53	dns	alert	4019988	medium
10/07 10:39:34	spyware	Suspicious DNS Query (generic:dtam.surelypercent838.ru)	TAP_MEN	TAP_MEN	10.1.145.119	192.168.30.40	53	dns	alert	4019988	medium
10/07 10:39:30	spyware	Suspicious DNS Query (generic:dtam.surelypercent838.ru)	TAP_MEN	TAP_MEN	10.1.145.119	10.1.1.173	53	dns	alert	4019988	medium
10/07 10:39:28	spyware	Suspicious DNS Query (generic:dtam.surelypercent838.ru)	TAP_MEN	TAP_MEN	10.1.145.119	192.168.30.40	53	dns	alert	4019988	medium
10/07 10:39:24	spyware	Suspicious DNS Query (generic:dtam.surelypercent838.ru)	TAP_MEN	TAP_MEN	10.1.145.119	10.1.1.173	53	dns	alert	4019988	medium
10/07 10:39:15	spyware	Suspicious DNS Query (generic:dtam.surelypercent838.ru)	TAP_MEN	TAP_MEN	10.1.145.119	192.168.30.40	53	dns	alert	4019988	medium
10/07 10:39:11	spyware	Suspicious DNS Query (generic:dtam.surelypercent838.ru)	TAP_MEN	TAP_MEN	10.1.145.119	10.1.1.173	53	dns	alert	4019988	medium
10/07 10:39:09	spyware	Suspicious DNS Query (generic:dtam.surelypercent838.ru)	TAP_MEN	TAP_MEN	10.1.145.119	192.168.30.40	53	dns	alert	4019988	medium
10/07 10:39:05	spyware	Suspicious DNS Query (generic:dtam.surelypercent838.ru)	TAP_MEN	TAP_MEN	10.1.145.119	10.1.1.173	53	dns	alert	4019988	medium
10/07 10:38:54	spyware	Suspicious DNS Query (generic:dtam.surelypercent838.ru)	TAP_MEN	TAP_MEN	10.1.145.119	192.168.30.40	53	dns	alert	4019988	medium

Fuente: Logs NGFW CAN.

Para la IP 10.1.145.64 con nombre equipo zriano:

Figura 26. Detección de amenaza - miércoles 12/10/2016



(addr.src in 10.1.145.64) and (severity neq informational)

Receive Time	Type	Name	From Zone	To Zone	Attacker	Victim	To Port	Application	Action	ID	Severity
10/07 15:07:27	spyware	Suspicious DNS Query (generic:dtam.surelypercent838.ru)	TAP_DMZ	TAP_DMZ	10.1.145.64	192.168.30.40	53	dns	alert	4019988	medium
10/07 15:07:23	spyware	Suspicious DNS Query (generic:dtam.surelypercent838.ru)	TAP_DMZ	TAP_DMZ	10.1.145.64	10.1.1.173	53	dns	alert	4019988	medium
10/07 15:07:21	spyware	Suspicious DNS Query (generic:dtam.surelypercent838.ru)	TAP_DMZ	TAP_DMZ	10.1.145.64	192.168.30.40	53	dns	alert	4019988	medium
10/07 15:07:15	spyware	Suspicious DNS Query (generic:dtam.surelypercent838.ru)	TAP_DMZ	TAP_DMZ	10.1.145.64	192.168.30.40	53	dns	alert	4019988	medium
10/07 15:07:15	spyware	Suspicious DNS Query (generic:dtam.surelypercent838.ru)	TAP_DMZ	TAP_DMZ	10.1.145.64	10.1.1.173	53	dns	alert	4019988	medium
10/07 15:07:08	spyware	Suspicious DNS Query (generic:dtam.surelypercent838.ru)	TAP_DMZ	TAP_DMZ	10.1.145.64	10.1.1.173	53	dns	alert	4019988	medium
10/07 15:07:07	spyware	Suspicious DNS Query (generic:dtam.surelypercent838.ru)	TAP_DMZ	TAP_DMZ	10.1.145.64	192.168.30.40	53	dns	alert	4019988	medium
10/07 09:20:42	spyware	Suspicious DNS Query (generic:dtam.surelypercent838.ru)	TAP_DMZ	TAP_DMZ	10.1.145.64	192.168.30.40	53	dns	alert	4019988	medium
10/07 09:20:42	spyware	Suspicious DNS Query (generic:dtam.surelypercent838.ru)	TAP_DMZ	TAP_DMZ	10.1.145.64	10.1.1.173	53	dns	alert	4019988	medium
10/07 09:20:35	spyware	Suspicious DNS Query (generic:dtam.surelypercent838.ru)	TAP_DMZ	TAP_DMZ	10.1.145.64	192.168.30.40	53	dns	alert	4019988	medium
10/07 09:20:34	spyware	Suspicious DNS Query (generic:dtam.surelypercent838.ru)	TAP_DMZ	TAP_DMZ	10.1.145.64	10.1.1.173	53	dns	alert	4019988	medium
10/07 09:20:26	spyware	Suspicious DNS Query (generic:dtam.surelypercent838.ru)	TAP_DMZ	TAP_DMZ	10.1.145.64	192.168.30.40	53	dns	alert	4019988	medium
10/07 09:20:19	spyware	Suspicious DNS Query (generic:dtam.surelypercent838.ru)	TAP_DMZ	TAP_DMZ	10.1.145.64	192.168.30.40	53	dns	alert	4019988	medium
10/07 09:20:19	spyware	Suspicious DNS Query (generic:dtam.surelypercent838.ru)	TAP_DMZ	TAP_DMZ	10.1.145.64	10.1.1.173	53	dns	alert	4019988	medium
10/07 09:20:12	spyware	Suspicious DNS Query (generic:dtam.surelypercent838.ru)	TAP_DMZ	TAP_DMZ	10.1.145.64	10.1.1.173	53	dns	alert	4019988	medium
10/07 09:20:11	spyware	Suspicious DNS Query (generic:dtam.surelypercent838.ru)	TAP_DMZ	TAP_DMZ	10.1.145.64	192.168.30.40	53	dns	alert	4019988	medium
10/07 07:57:44	vulnerability	Microsoft Windows Date and Time Enumeration	TAP_DMZ	TAP_DMZ	10.1.145.64	10.1.1.173	445	ms-ds-smb	alert	30841	low
10/07 07:57:15	vulnerability	Windows Local Security Architect lsardelete access	TAP_DMZ	TAP_DMZ	10.1.145.64	10.1.1.173	1028	active-directory	alert	30857	low
10/06 16:47:53	spyware	Suspicious DNS Query (generic:dtam.surelypercent838.ru)	TAP_DMZ	TAP_DMZ	10.1.145.64	10.1.1.173	53	dns	alert	4019988	medium
10/06 16:47:52	spyware	Suspicious DNS Query (generic:dtam.surelypercent838.ru)	TAP_DMZ	TAP_DMZ	10.1.145.64	192.168.30.40	53	dns	alert	4019988	medium
10/06 16:47:47	spyware	Suspicious DNS Query (generic:dtam.surelypercent838.ru)	TAP_DMZ	TAP_DMZ	10.1.145.64	10.1.1.173	53	dns	alert	4019988	medium
10/06 16:47:46	spyware	Suspicious DNS Query (generic:dtam.surelypercent838.ru)	TAP_DMZ	TAP_DMZ	10.1.145.64	192.168.30.40	53	dns	alert	4019988	medium
10/06 16:45:04	spyware	Suspicious DNS Query (generic:dtam.surelypercent838.ru)	TAP_DMZ	TAP_DMZ	10.1.145.64	10.1.1.173	53	dns	alert	4019988	medium
10/06 16:44:58	spyware	Suspicious DNS Query (generic:dtam.surelypercent838.ru)	TAP_DMZ	TAP_DMZ	10.1.145.64	192.168.30.40	53	dns	alert	4019988	medium
10/06 16:44:57	spyware	Suspicious DNS Query (generic:dtam.surelypercent838.ru)	TAP_DMZ	TAP_DMZ	10.1.145.64	10.1.1.173	53	dns	alert	4019988	medium
10/06 16:44:52	spyware	Suspicious DNS Query (generic:dtam.surelypercent838.ru)	TAP_DMZ	TAP_DMZ	10.1.145.64	192.168.30.40	53	dns	alert	4019988	medium
10/06 16:44:48	spyware	Suspicious DNS Query (generic:dtam.surelypercent838.ru)	TAP_DMZ	TAP_DMZ	10.1.145.64	10.1.1.173	53	dns	alert	4019988	medium

Fuente: Logs NGFW CAN.

- **Detección de amenaza - jueves 27/10/2016**

Solicito por favor se realice la revisión si tienen instalado el paquete antivirus sobre el *endpoints* de mbojaca y ejalvarado, si tiene instalado el paquete antivirus por favor realizar actualización de la base de datos y lanzar un escaneo total, ya que producto del análisis de logs de los NGFW Palo Alto, se evidenció que se está generando tráfico tipo "*spyware*" reenviando múltiples solicitudes del dominio duckdns4.duckdns.org y se tienen altos indicios de estar infectados como se evidencia en la figura 27 y 28.

Para la IP 10.1.110.150 con nombre equipo mbojaca:

Figura 27. Detección de amenaza - jueves 27/10/2016

Receive Time	Type	Name	From Zone	To Zone	Attacker	Victim	To Port	Application	Action	ID	Severity
10/25 17:52:47	spyware	generic:duckdns4.duckdns.org	TAP_MEN	TAP_MEN	10.1.110.150	192.168.30.40	53	dns	alert	3816979	medium
10/25 17:52:47	spyware	generic:duckdns4.duckdns.org	TAP_MEN	TAP_MEN	10.1.110.150	10.1.1.173	53	dns	alert	3816979	medium
10/25 17:52:41	spyware	generic:duckdns4.duckdns.org	TAP_MEN	TAP_MEN	10.1.110.150	10.1.1.173	53	dns	alert	3816979	medium
10/25 17:52:40	spyware	generic:duckdns4.duckdns.org	TAP_MEN	TAP_MEN	10.1.110.150	192.168.30.40	53	dns	alert	3816979	medium
10/25 17:52:30	spyware	generic:duckdns4.duckdns.org	TAP_MEN	TAP_MEN	10.1.110.150	10.1.1.173	53	dns	alert	3816979	medium
10/25 17:52:30	spyware	generic:duckdns4.duckdns.org	TAP_MEN	TAP_MEN	10.1.110.150	192.168.30.40	53	dns	alert	3816979	medium
10/25 17:52:24	spyware	generic:duckdns4.duckdns.org	TAP_MEN	TAP_MEN	10.1.110.150	10.1.1.173	53	dns	alert	3816979	medium
10/25 17:52:23	spyware	generic:duckdns4.duckdns.org	TAP_MEN	TAP_MEN	10.1.110.150	192.168.30.40	53	dns	alert	3816979	medium
10/25 17:52:14	spyware	generic:duckdns4.duckdns.org	TAP_MEN	TAP_MEN	10.1.110.150	192.168.30.40	53	dns	alert	3816979	medium
10/25 17:52:14	spyware	generic:duckdns4.duckdns.org	TAP_MEN	TAP_MEN	10.1.110.150	10.1.1.173	53	dns	alert	3816979	medium
10/25 17:52:08	spyware	generic:duckdns4.duckdns.org	TAP_MEN	TAP_MEN	10.1.110.150	10.1.1.173	53	dns	alert	3816979	medium
10/25 17:52:07	spyware	generic:duckdns4.duckdns.org	TAP_MEN	TAP_MEN	10.1.110.150	192.168.30.40	53	dns	alert	3816979	medium
10/25 17:51:58	spyware	generic:duckdns4.duckdns.org	TAP_MEN	TAP_MEN	10.1.110.150	192.168.30.40	53	dns	alert	3816979	medium
10/25 17:51:58	spyware	generic:duckdns4.duckdns.org	TAP_DMZ	TAP_DMZ	10.1.110.150	10.1.1.173	53	dns	alert	3816979	medium
10/25 17:51:52	spyware	generic:duckdns4.duckdns.org	TAP_MEN	TAP_MEN	10.1.110.150	10.1.1.173	53	dns	alert	3816979	medium
10/25 17:51:51	spyware	generic:duckdns4.duckdns.org	TAP_MEN	TAP_MEN	10.1.110.150	192.168.30.40	53	dns	alert	3816979	medium
10/25 17:51:42	spyware	generic:duckdns4.duckdns.org	TAP_MEN	TAP_MEN	10.1.110.150	10.1.1.173	53	dns	alert	3816979	medium
10/25 17:51:42	spyware	generic:duckdns4.duckdns.org	TAP_MEN	TAP_MEN	10.1.110.150	192.168.30.40	53	dns	alert	3816979	medium
10/25 17:51:36	spyware	generic:duckdns4.duckdns.org	TAP_MEN	TAP_MEN	10.1.110.150	10.1.1.173	53	dns	alert	3816979	medium
10/25 17:51:35	spyware	generic:duckdns4.duckdns.org	TAP_MEN	TAP_MEN	10.1.110.150	192.168.30.40	53	dns	alert	3816979	medium
10/25 17:51:26	spyware	generic:duckdns4.duckdns.org	TAP_MEN	TAP_MEN	10.1.110.150	192.168.30.40	53	dns	alert	3816979	medium
10/25 17:51:26	spyware	generic:duckdns4.duckdns.org	TAP_MEN	TAP_MEN	10.1.110.150	10.1.1.173	53	dns	alert	3816979	medium
10/25 17:51:20	spyware	generic:duckdns4.duckdns.org	TAP_MEN	TAP_MEN	10.1.110.150	10.1.1.173	53	dns	alert	3816979	medium
10/25 17:51:19	spyware	generic:duckdns4.duckdns.org	TAP_MEN	TAP_MEN	10.1.110.150	192.168.30.40	53	dns	alert	3816979	medium
10/25 17:51:10	spyware	generic:duckdns4.duckdns.org	TAP_MEN	TAP_MEN	10.1.110.150	192.168.30.40	53	dns	alert	3816979	medium

Fuente: Logs NGFW CAN.

Para la IP 10.1.110.160 con nombre equipo ejalvarado:

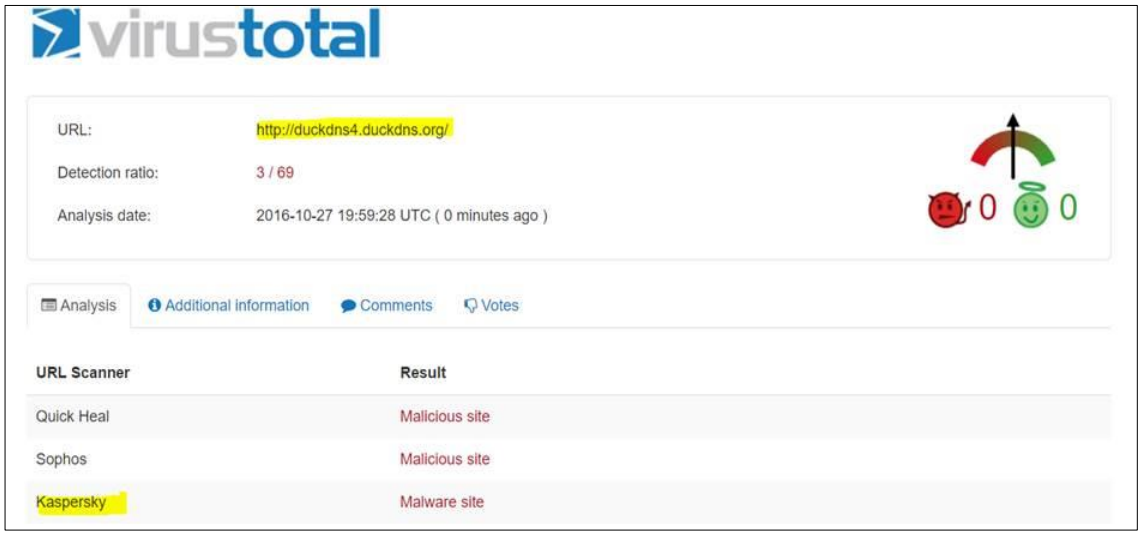
Figura 28. Detección de amenaza - jueves 27/10/2016

Receive Time	Type	Name	From Zone	To Zone	Attacker	Victim	To Port	Application	Action	ID	Severity
10/26 17:58:32	spyware	generic:duckdns4.duckdns.org	TAP_MEN	TAP_MEN	10.1.110.160	192.168.30.40	53	dns	alert	3816979	medium
10/26 17:58:32	spyware	generic:duckdns4.duckdns.org	TAP_DMZ	TAP_DMZ	10.1.110.160	10.1.1.173	53	dns	alert	3816979	medium
10/26 17:58:26	spyware	generic:duckdns4.duckdns.org	TAP_MEN	TAP_MEN	10.1.110.160	192.168.30.40	53	dns	alert	3816979	medium
10/26 17:58:25	spyware	generic:duckdns4.duckdns.org	TAP_MEN	TAP_MEN	10.1.110.160	10.1.1.173	53	dns	alert	3816979	medium
10/26 17:58:16	spyware	generic:duckdns4.duckdns.org	TAP_MEN	TAP_MEN	10.1.110.160	10.1.1.173	53	dns	alert	3816979	medium
10/26 17:58:16	spyware	generic:duckdns4.duckdns.org	TAP_MEN	TAP_MEN	10.1.110.160	192.168.30.40	53	dns	alert	3816979	medium
10/26 17:58:10	spyware	generic:duckdns4.duckdns.org	TAP_MEN	TAP_MEN	10.1.110.160	192.168.30.40	53	dns	alert	3816979	medium
10/26 17:58:09	spyware	generic:duckdns4.duckdns.org	TAP_MEN	TAP_MEN	10.1.110.160	10.1.1.173	53	dns	alert	3816979	medium
10/26 17:58:00	spyware	generic:duckdns4.duckdns.org	TAP_MEN	TAP_MEN	10.1.110.160	10.1.1.173	53	dns	alert	3816979	medium
10/26 17:58:00	spyware	generic:duckdns4.duckdns.org	TAP_MEN	TAP_MEN	10.1.110.160	192.168.30.40	53	dns	alert	3816979	medium
10/26 17:57:54	spyware	generic:duckdns4.duckdns.org	TAP_MEN	TAP_MEN	10.1.110.160	192.168.30.40	53	dns	alert	3816979	medium
10/26 17:57:53	spyware	generic:duckdns4.duckdns.org	TAP_MEN	TAP_MEN	10.1.110.160	10.1.1.173	53	dns	alert	3816979	medium
10/26 17:57:44	spyware	generic:duckdns4.duckdns.org	TAP_MEN	TAP_MEN	10.1.110.160	192.168.30.40	53	dns	alert	3816979	medium
10/26 17:57:44	spyware	generic:duckdns4.duckdns.org	TAP_MEN	TAP_MEN	10.1.110.160	10.1.1.173	53	dns	alert	3816979	medium
10/26 17:57:38	spyware	generic:duckdns4.duckdns.org	TAP_MEN	TAP_MEN	10.1.110.160	192.168.30.40	53	dns	alert	3816979	medium
10/26 17:57:37	spyware	generic:duckdns4.duckdns.org	TAP_MEN	TAP_MEN	10.1.110.160	10.1.1.173	53	dns	alert	3816979	medium
10/26 17:57:28	spyware	generic:duckdns4.duckdns.org	TAP_MEN	TAP_MEN	10.1.110.160	192.168.30.40	53	dns	alert	3816979	medium
10/26 17:57:28	spyware	generic:duckdns4.duckdns.org	TAP_MEN	TAP_MEN	10.1.110.160	10.1.1.173	53	dns	alert	3816979	medium
10/26 17:57:22	spyware	generic:duckdns4.duckdns.org	TAP_MEN	TAP_MEN	10.1.110.160	192.168.30.40	53	dns	alert	3816979	medium
10/26 17:57:21	spyware	generic:duckdns4.duckdns.org	TAP_MEN	TAP_MEN	10.1.110.160	10.1.1.173	53	dns	alert	3816979	medium
10/26 17:57:11	spyware	generic:duckdns4.duckdns.org	TAP_MEN	TAP_MEN	10.1.110.160	192.168.30.40	53	dns	alert	3816979	medium
10/26 17:57:11	spyware	generic:duckdns4.duckdns.org	TAP_DMZ	TAP_DMZ	10.1.110.160	10.1.1.173	53	dns	alert	3816979	medium
10/26 17:57:05	spyware	generic:duckdns4.duckdns.org	TAP_MEN	TAP_MEN	10.1.110.160	192.168.30.40	53	dns	alert	3816979	medium
10/26 17:57:04	spyware	generic:duckdns4.duckdns.org	TAP_MEN	TAP_MEN	10.1.110.160	10.1.1.173	53	dns	alert	3816979	medium
10/26 17:56:55	spyware	generic:duckdns4.duckdns.org	TAP_MEN	TAP_MEN	10.1.110.160	10.1.1.173	53	dns	alert	3816979	medium

Fuente: Logs NGFW CAN.

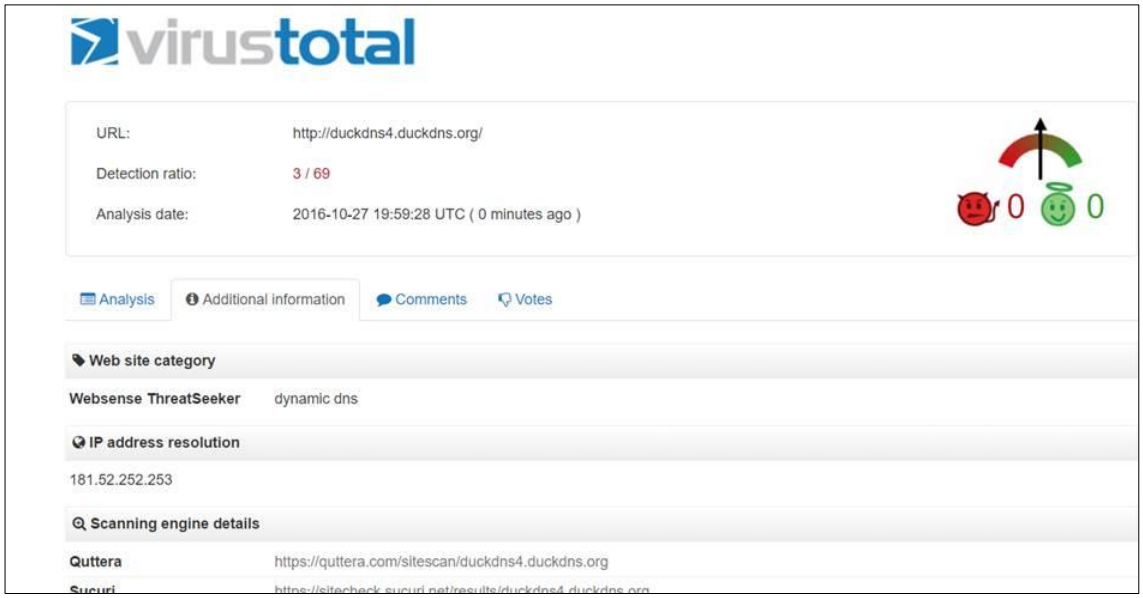
Se valida el dominio http://duckdns4.duckdns.org/ en virustotal:

Figura 29. Carga del dominio malicioso http://duckdns4.duckdns.org en virustotal



Fuente: Sitio web de VirusTotal (www.virustotal.com).

Figura 30. Información adicional del dominio malicioso http://duckdns4.duckdns.orf en virustotal



Fuente: Sitio web de VirusTotal (www.virustotal.com).

ANEXO C. REPORTES MENSUALES NGFW Y WAF

Para las gráficas del anexo c, las barras de color azul indican que la firmas están permitidas y las barras de color rojo indican que la firmas se encuentran bloqueadas, para las firmas que tienen las dos barras la azul y roja de manera simultáneamente, indica que en ese mes se activó el bloqueo por lo que existe un tráfico permitido y otro bloqueado.

Para la sede de Diveo no se observa gráficas de anti-virus ni de anti-spyware debido a que en esta sede se encuentran los servidores de producción y desarrollo, por tal motivo a nivel de firewall perimetral cuentan con accesos restringidos bajo la política “Todo cerrado excepto” por lo tanto no tiene registros de eventos de estos dos módulos, a diferencia de la sede de CAN donde se cuenta con el acceso a todos los usuarios del MEN y adicionalmente también cuentas con una zona de servidores con los ambientes de pruebas, desarrollo y producción.

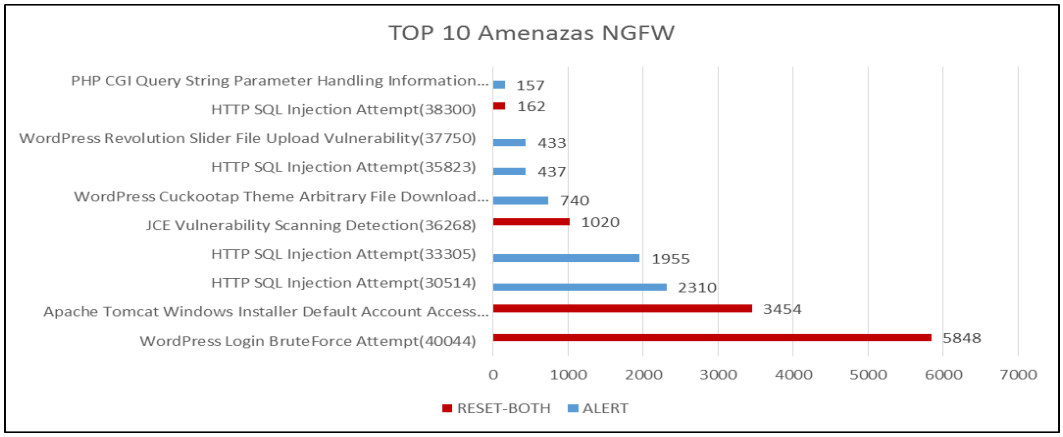
A continuación, se observan los reportes desde el mes de mayo a diciembre de 2016:

C.1 Reporte mensual estadístico NGFW y WAF – Mayo

DIVEO NGFW

- **Top de amenazas por firma**

Gráfica 26. Top 10 amenazas NGFW DIVEO - mayo 2016

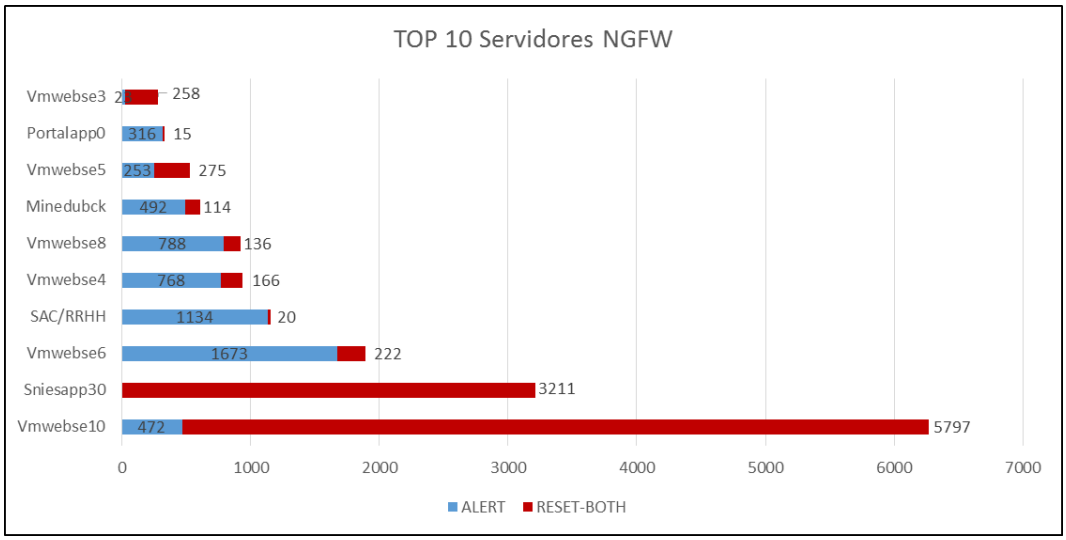


Fuente: Logs NGFW DIVEO mes de mayo 2016.

Como se observa en la gráfica 26, las 3 firmas con mayor número de eventos son: *"WordPress Login BruteForce Attempt (40044), Apache Tomcat Windows Installer Default Account Access Vulnerability (34160)" y HTTP SQL Injection Attempt (30514)"* con el 33.63%, 19.86% y 13.29% respectivamente del total de eventos detectados, donde las barras azules representan los eventos permitidos y las barras de color rojo los eventos bloqueados catalogados como amenazas.

- **Top de servidores con más eventos**

Gráfica 27. Top servidores con más eventos NGFW DIVEO - mayo 2016

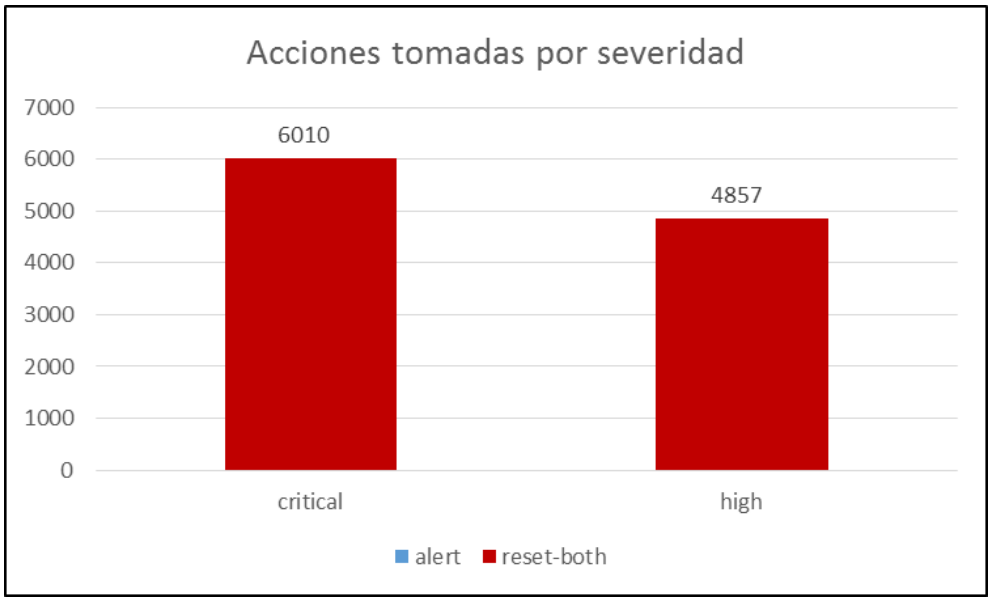


Fuente: Logs NGFW DIVEO mes de mayo 2016.

Como se observa en la gráfica 27, los 3 servidores con mayor número de eventos son: *"Vmwebse10"* con el 36.05%, *"Sniesapp30"* con el 18.47% *y "Vmwebse6"* con el 10.9% del total de eventos detectados, donde las barras azules representan las firmas permitidas y las barras de color rojo las firmas bloqueadas identificadas como amenazas.

- **Acciones por severidad *critical* y *high***

Gráfica 28. Acciones tomadas por severidad NGFW DIVEO - mayo 2016



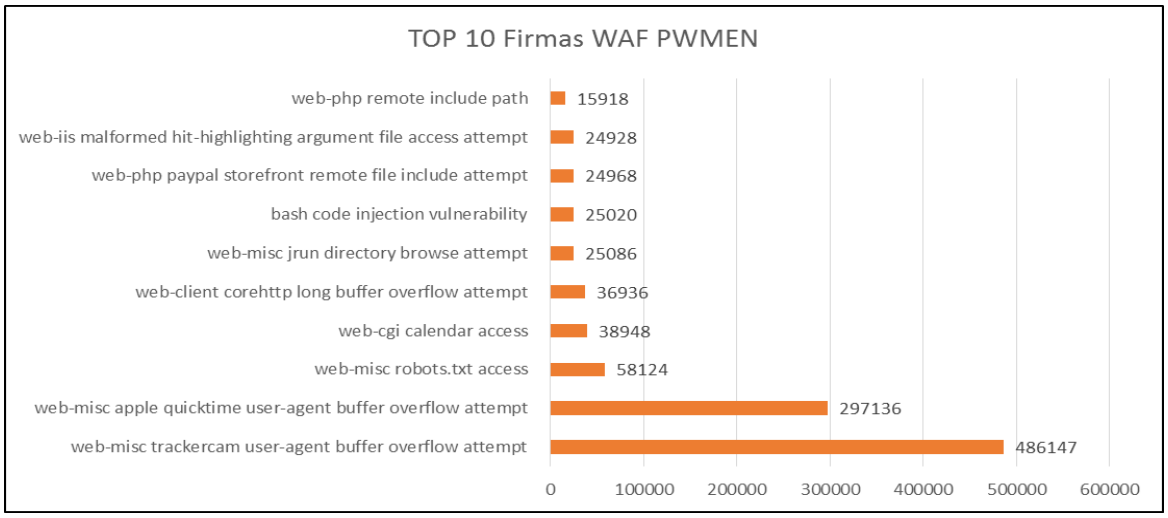
Fuente: Logs NGFW DIVEO mes de mayo 2016.

Como se observa en la gráfica 28, el 100% de las amenazas con severidades *critical* y *high* están siendo bloqueadas en el NGFW de la sede de DIVEO.

DIVEO WAF

- **Top amenazas por firmas**

Gráfica 29. Top 10 firmas WAF - mayo 2016

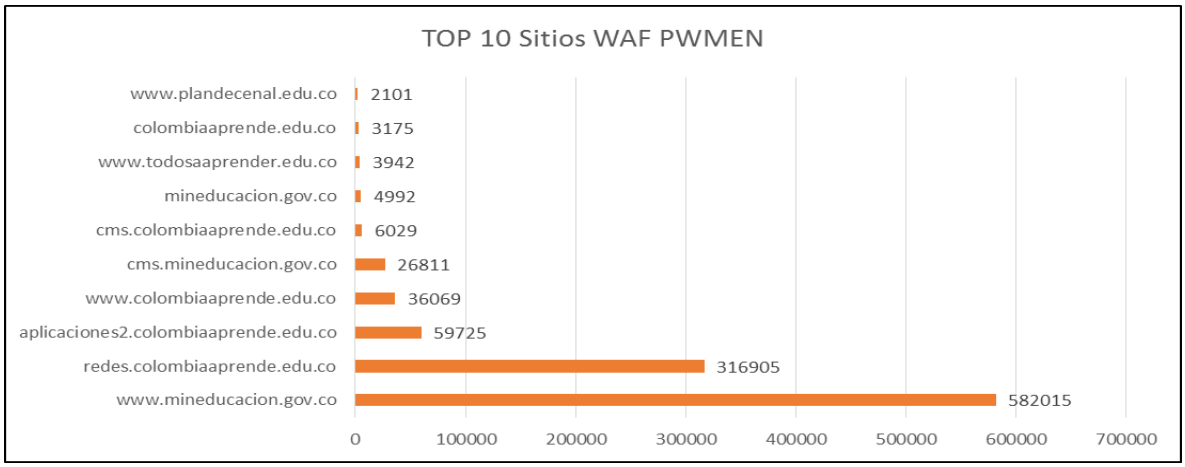


Fuente: Logs WAF mes de mayo 2016.

Como se observa en la gráfica 29, las 3 firmas con mayor número de eventos son: *"web-misc trackercam user-agent buffer overflow attempt, web-misc apple quicktime user-agent buffer overflow attempt y web-misc robots.txt access",* con el 46.44%, 28.38% y 5.55% respectivamente del total de eventos presentados.

- **Top sitios web con más eventos**

Gráfica 30. Top 10 sitios WAF - mayo 2016

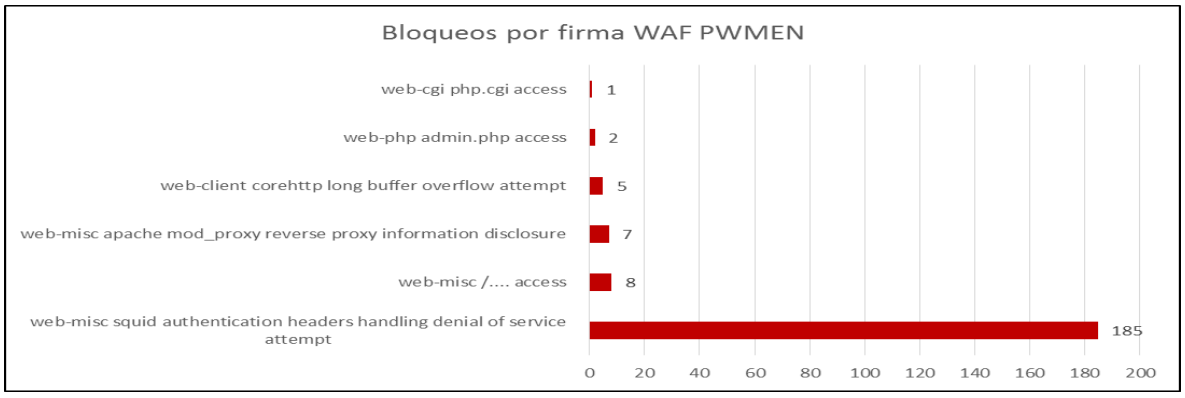


Fuente: Logs WAF mes de mayo 2016.

Los 3 sitios web con mayor número de eventos de acuerdo a la gráfica 30 son: *"www.mineducacion.gov.co"* con el 55.59%, *"redes.colombiaaprende.edu.co"* con el 30.27%, *y "aplicaciones2.colombiaaprende.edu.co"* con el 5.7% del total de eventos presentados.

- **Top bloqueo por firmas**

Gráfica 31. Bloqueo por firmas WAF – mayo 2016

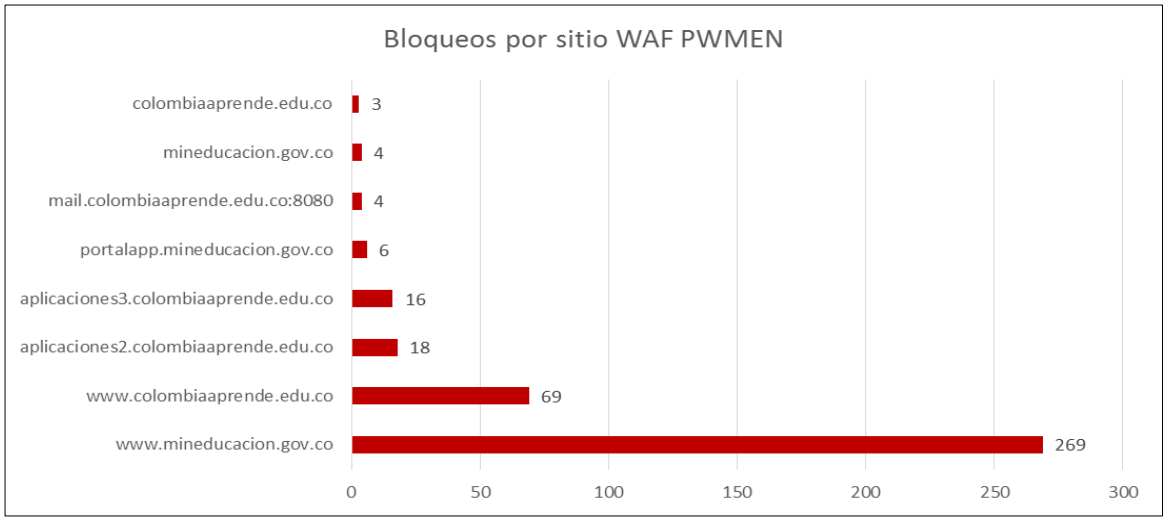


Fuente: Logs WAF mes de mayo 2016.

Las 3 firmas con mayor número de bloqueos de acuerdo a la gráfica 31 identificadas como amenazas son: *"web-mis squid authentications headers handing denial of service attemmpt, web-misc/Access y web-mis apache mod_proxy reverse information disclousure"* con un 89%, 4% y 3,5% respectivamente del total de eventos presentados.

- **Top bloqueo por sitios**

Gráfica 32. Bloqueo por sitio WAF – mayo 2016



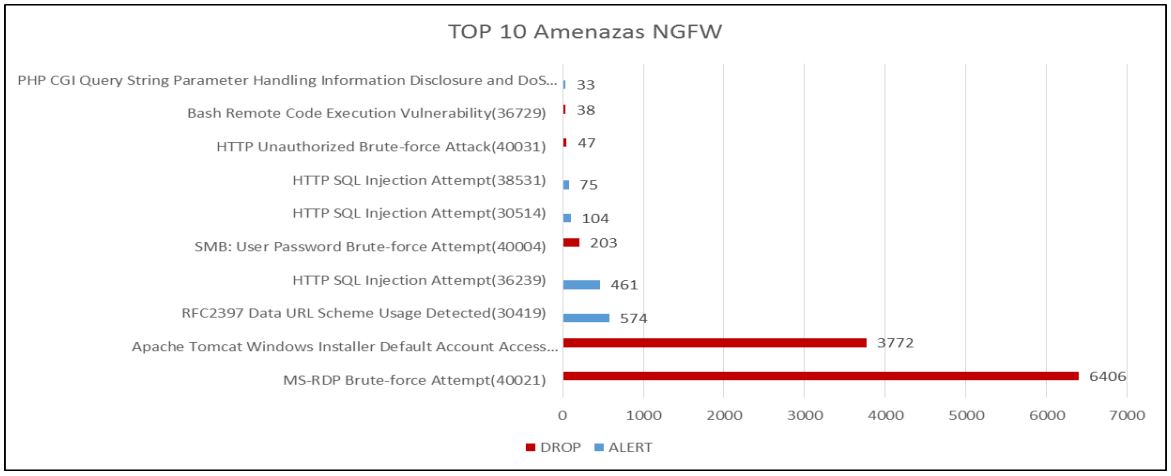
Fuente: Logs WAF mes de mayo 2016.

Los 3 sitios web con mayor número de firmas bloqueadas identificadas como amenazas de acuerdo a la gráfica 32 son: *"www.mineducacion.gov.co", "www.colombiaaprende.edu.co"* y *"aplicaciones2.colombiaaprende.edu.co"* correspondiente al 69%, 18% y 4% respectivamente del total de firmas bloqueadas.

CAN NGFW

- **Top de amenazas por firma**

Gráfica 33. Fuente: Logs NGFW CAN - mayo 2016

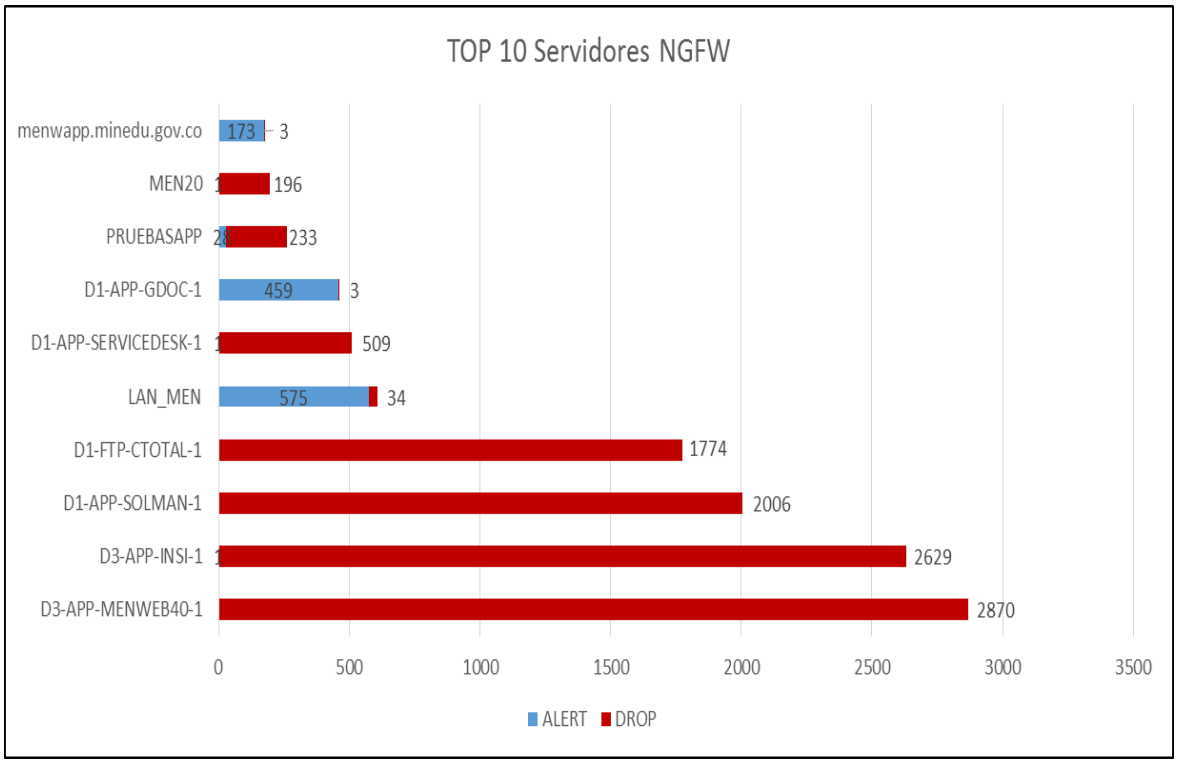


Fuente: Logs NGFW CAN mes de mayo 2016.

Como se observa en la gráfica 33, las 3 firmas con mayor número de eventos son: *"MS-RDP Brute-force Attempt (40021), Apache Tomcat Windows Installer Default Account Access Vulnerability (34160) y RFC2397 Data URL Scheme Usage Detected (30419),* con el 53.67%, 31.6% y 4.81% respectivamente del total de eventos detectadas, donde las barras azules representan los eventos permitidos y las barras de color rojo los eventos bloqueados catalogados como amenazas.

➢ **Top de servidores con más eventos**

Gráfica 34. Top servidores con más eventos NGFW CAN - mayo 2016

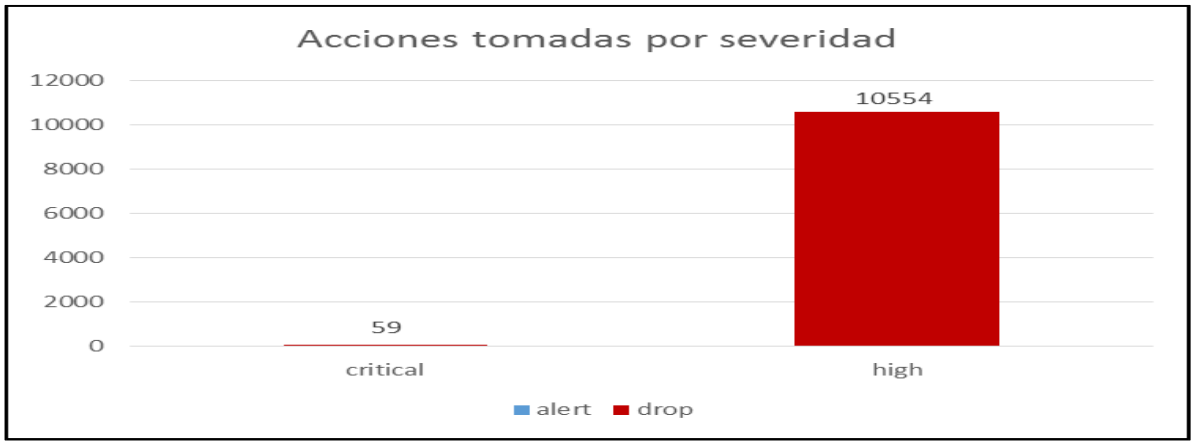


Fuente: Logs NGFW CAN mes de mayo 2016.

Como se observa en la gráfica 34, los 3 servidores con mayor número de eventos son: *"D3-APP-MENWEB40-1"* con el 24.04%, *"D3-APP-INSI-1"* con el 22.03%, y *"D1-APP-SOLMAN-1"* con el 16.8% del total de eventos detectados, donde las barras azules representan las firmas permitidas y las barras de color rojo las firmas bloqueadas identificadas como amenazas.

- **Acciones por severidad *critical* y *high***

Gráfica 35. Acciones tomadas por severidad NGFW CAN - mayo 2016



Fuente: Logs NGFW CAN mes de mayo 2016.

Como se observa en la gráfica 35, el 100% de las amenazas con severidades *critical* y *high* están siendo bloqueadas en el NGFW de la sede del CAN.

- **Anti-Virus**

Cuadro 10. Eventos de anti-virus registrado en l el NGFW CAN – mayo 2016

Firma virus	Eventos
Virus/Win32.ramnit.fwlhz (2306876)	9
Virus/Win32.WGeneric.imaov (2116762)	5
Worm/Win32.rimecud.fszn (2334657)	5
Virus/Win32.WGeneric.hvswh (2043899)	4
Net-Worm/Win32.allaple.quqq (2786564)	3
Trojan/Win32.finb.oj(2402101)	1
Trojan/Win32.iframe.fbe (1270026)	1
Trojan/Win32.ramnit.ehhiu (2067873)	1
Virus/Win32.WGeneric.ilnbm (2433019)	1
Total	**30**

Fuente: Logs NGFW CAN mes de mayo 2016.

El 100% de las firmas detectadas por el módulo de anti-virus que se observan en el cuadro 10 fueron bloqueadas.

- **Anti-Spyware**

Cuadro 11. Eventos de anti-spyware registrado en l el NGFW CAN – mayo 2016

Firma spyware	Eventos
Sipvicious.Gen User-Agent Traffic (13272)	147025
Xtreme Rat.Gen Command and Control Traffic (13391)	23837
Morto RDP Request Traffic (13274)	18042
generic:psxyrgfwwcm.info(3802017)	4314
Suspicious DNS Query (generic:froveries.top) (4099781)	1266
generic:meinv.tv(3815418)	804
TrojanDownloader.dofoil:galatardoreal.com(3807237)	513
VirTool.ceeinject:gowentgone.eu(3807424)	507
generic:waxawj.net(3806312)	444
generic:xjervi.com(3807125)	443
Total	**270078**[49]
Fuente: Logs NGFW CAN mes de mayo 2016.	

Como se observa en el cuadro 11, las 3 firmas de anti-spyware con mayor número de eventos son: *"Sipvicious.Gen User-Agent Traffic (13272), Xtreme Rat.Gen Command and Control Traffic (13391) y Morto RDP Request Traffic (13274)"* con el 54.4%, 8.8% y 6.7% respectivamente del total de spyware detectado.

El 38.8% de eventos detectados dentro de esta categoría fueron bloqueados, con la configuración de defecto de bloqueo de la categoría *critical*.

[49] El total refleja la suma de todos los eventos asociados a las firmas de esta categoría y no solamente los mostrados en el TOP 10.

- **Eventos WildFire**

Cuadro 12. Eventos de Wildfire registrado en l el NGFW CAN – mayo 2016

Servidor	Microsoft office 2007 word document (52140)	Microsoft PE file (52060)	Windows Dynamic Link Library (DLL) (52019)	Windows executable (EXE) (52020)	Total general
IRONPORT	395	119	-	407	921
LAN_MEN	-	4	3	28	35
94232175201	-	2	-	9	11
162.144.249.75	-	4	-	5	9
208.115.223.30	-	-	-	9	9
50.28.39.32	-	3	-	6	9
194.90.9.19	-	-	-	8	8
95189106109	-	6	-	-	6
122.0.20.56	-	-	-	5	5
162.252.82.240	-	3	-	2	5
Total general	**395**	**145**	**3**	**549**	**1093**

Fuente: Logs NGFW CAN mes de mayo 2016.

Los archivos revisados por el sistema Wildfire, que se observan en el cuadro 12, son objetos con probabilidad de ser maliciosos, que son ejecutados y analizados en un entorno controlado. El sistema Wildfire realiza un diagnóstico, en donde si los archivos recientemente analizados se consideran maliciosos, se genera el reporte y se alimenta el repositorio de Palo Alto.

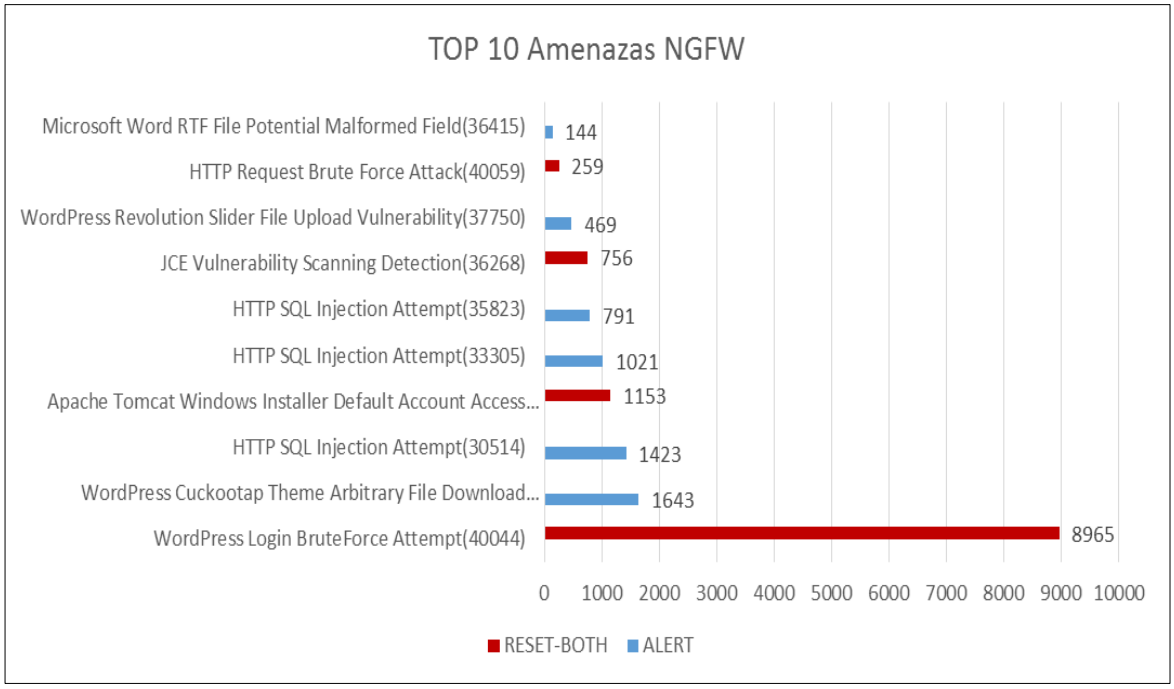
El 84.2% de los eventos diagnosticados por la nube de Palo Alto como "*malware*" o "*grayware*" se dirigieron por correo electrónico hacía el IronPort E-mail. Teniendo en cuenta esto se activó políticas de bloqueo de wildfire virus y se solicitó al área de sistemas operativos generar en el servidor Exchange políticas más estrictas para archivos adjuntos.

C.2 Reporte mensual estadístico NGFW y WAF – Junio

DIVEO NGFW

- **Top de amenazas por firma**

Gráfica 36. Top 10 amenazas NGFW DIVEO - junio 2016

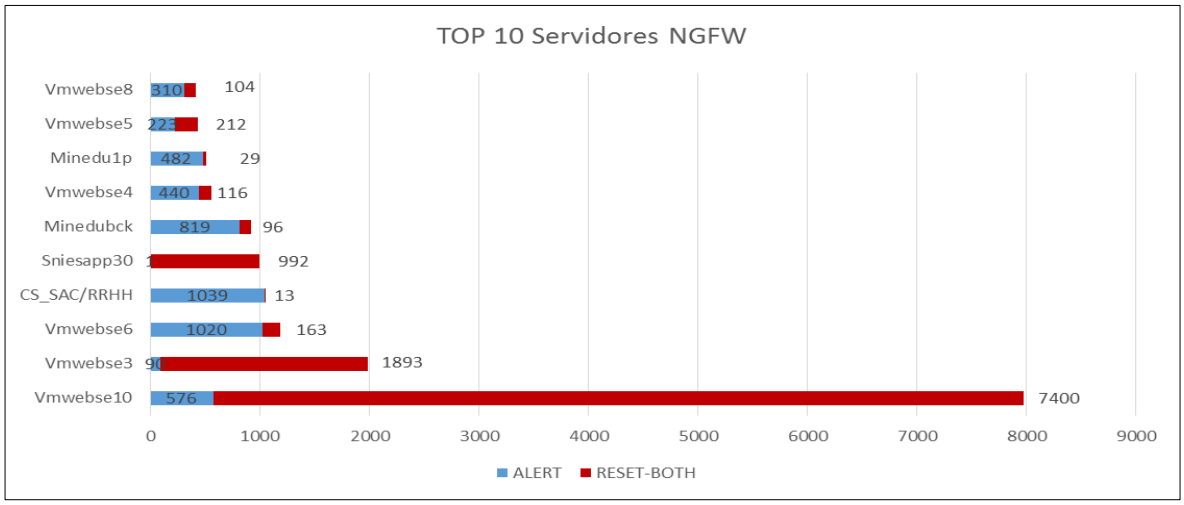


Fuente: Logs NGFW DIVEO mes de junio 2016.

Como se observa en la gráfica 36, las 3 firmas con mayor número de eventos son: *"WordPress Login BruteForce Attempt (40044), WordPress Cuckootap Theme Arbitrary File Download Vulnerability (37363) y HTTP SQL Injection Attempt (30514)" y* con el 49.8%, 9.1% y 7.4% respectivamente del total de firmas detectadas, donde las barras azules representan los eventos permitidos y las barras de color rojo los eventos bloqueados catalogados como amenazas.

➢ **Top de servidores con más eventos**

Gráfica 37. Top servidores con más eventos NGFW DIVEO - junio 2016

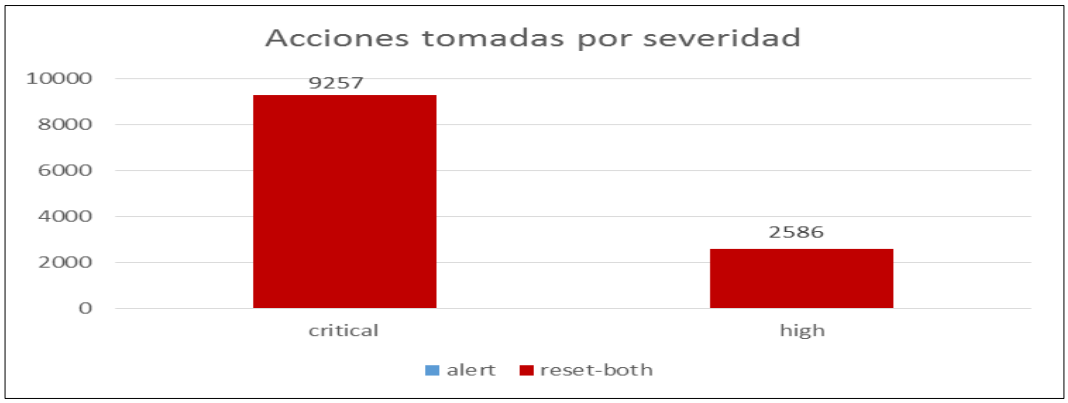


Fuente: Logs NGFW DIVEO mes de junio 2016.

Como se observa en la gráfica 37, los 3 servidores con mayor número de eventos son: *"Vmwebse10"* con el 44.08%, *"Vmwebse3"* con el 11.03% *y "Vmwebse6"* con el 6.58% del total de eventos detectados, donde las barras azules representan las firmas permitidas y las barras de color rojo las firmas bloqueadas identificadas como amenazas.

Acciones por severidad *critical* y *high*

Gráfica 38. Acciones tomadas por severidad NGFW DIVEO - junio 2016



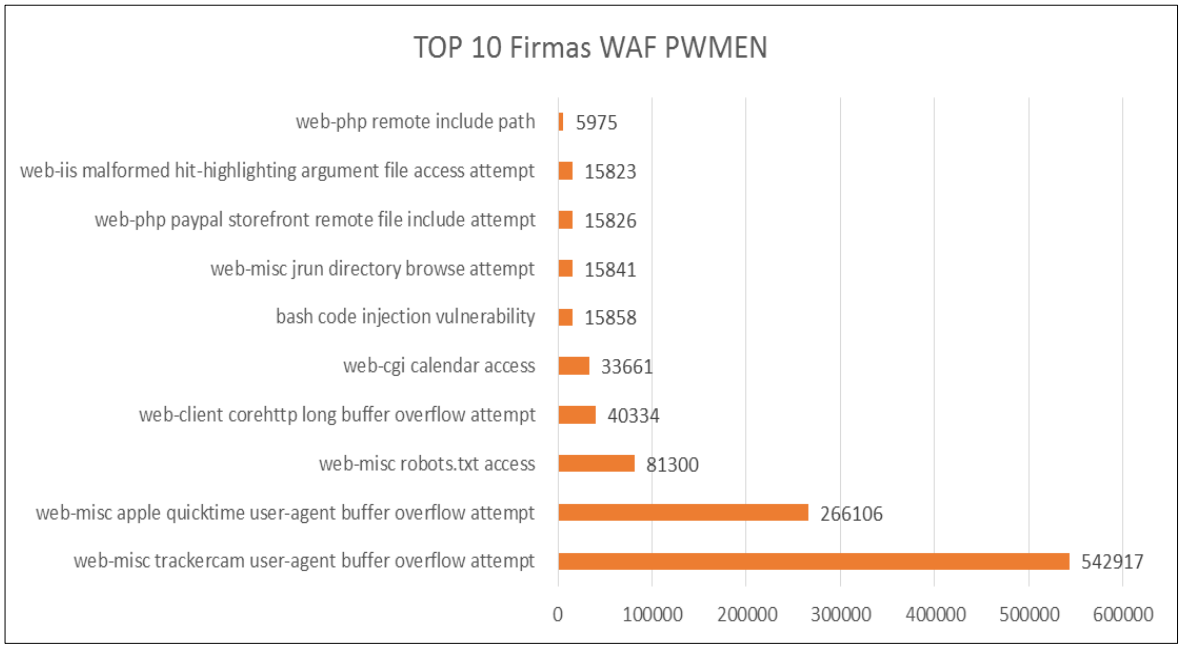
Fuente: Logs NGFW DIVEO mes de junio 2016.

Como se observa en la gráfica 38, el 100% de las amenazas con severidad *critical* y *high* están siendo bloqueadas en el NGFW de la sede de DIVEO.

DIVEO WAF

- **Top amenazas por firmas**

Gráfica 39. Top 10 firmas WAF - junio 2016

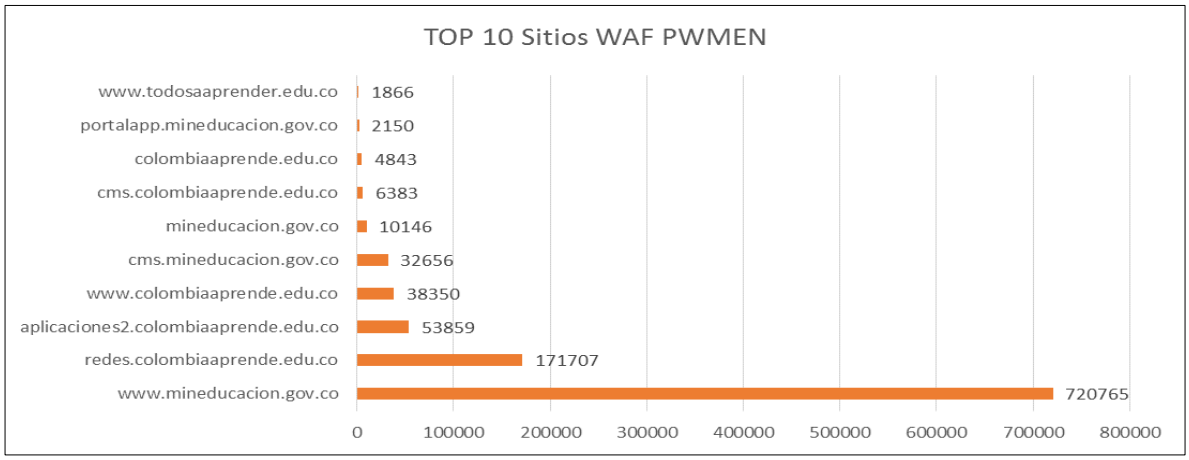


Fuente: Logs WAF mes de junio 2016.

Como se observa en la gráfica 39, las 3 firmas con mayor número de eventos son: *"web-misc trackercam user-agent buffer overflow attempt, web-misc apple quicktime user-agent buffer overflow attempt y web-misc robots.txt access",* con el 51.78%, 25.38% y 7.75% respectivamente del total de eventos presentados.

- **Top sitios web con más eventos**

Gráfica 40. Top 10 sitios WAF - junio 2016

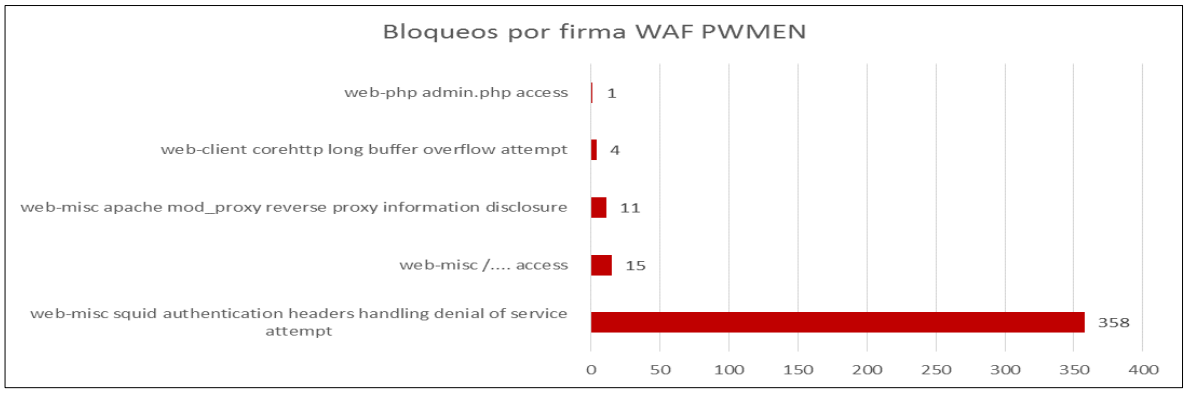


Fuente: Logs WAF mes de junio 2016.

Los 3 sitios web con mayor número de eventos, de acuerdo a la gráfica 40 son: *"www.mineducacion.gov.co"* con el 68.74%, *"redes.colombiaaprende.edu.co"* con el 16.38%, *y "aplicaciones2.colombiaaprende.edu.co"* con el 5.14% del total de eventos presentados.

- **Top bloqueo por firmas**

Gráfica 41. Bloqueo por firmas WAF – junio 2016

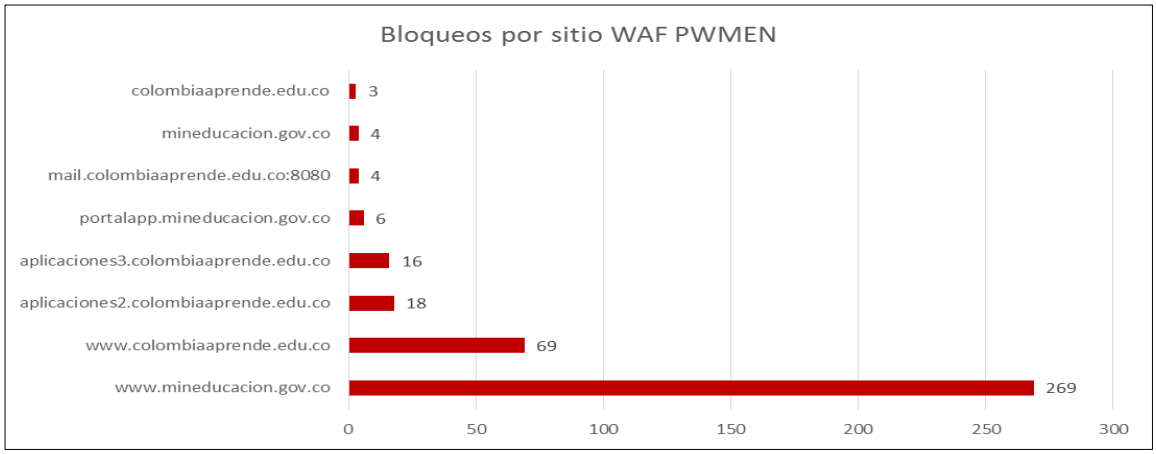


Fuente: Logs WAF mes de junio 2016.

Las 3 firmas con mayor número de bloqueos de acuerdo a la gráfica 41 identificadas como amenazas son: *"web-mis squid authentications headers handing denial of service attemmpt, web-misc/Access y web-mis apache mod_proxy reverse information disclousure"* con un 92%, 4% y 3,5% respectivamente del total de eventos presentados.

- **Top bloqueo por sitios**

Gráfica 42. Bloqueo por sitio WAF – junio 2016



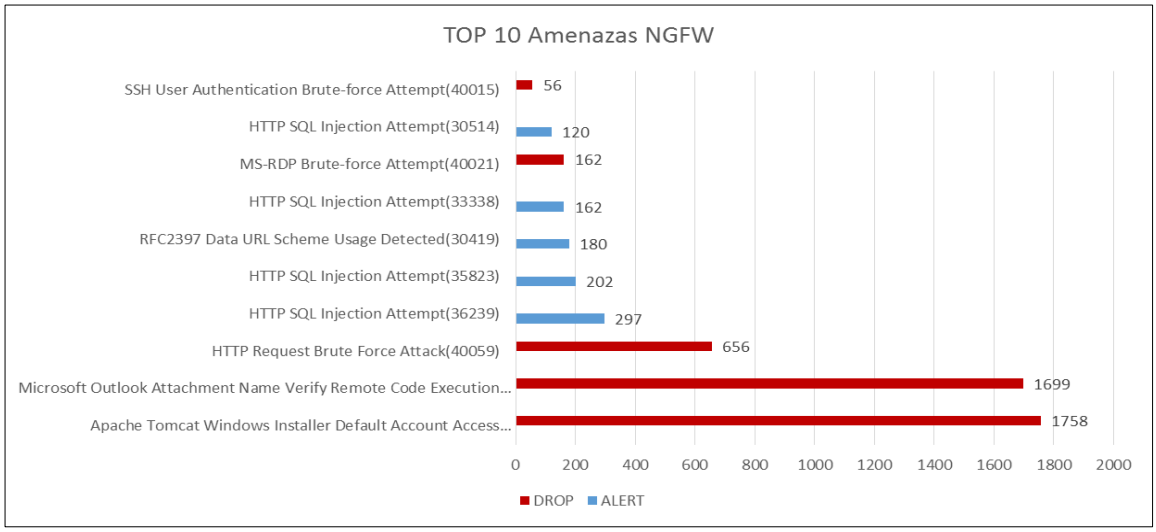
Fuente: Logs WAF mes de junio 2016.

Los 3 sitios web con mayor número de firmas bloqueadas identificadas como amenazas de acuerdo a la gráfica 42 son: *"www.mineducacion.gov.co"*, *"www.colombiaaprende.edu.co"* y *"aplicaciones2.colombiaaprende.edu.co"* correspondiente al 69%, 18% y 4% respectivamente del total de firmas bloqueadas.

CAN NGFW

- **Top de amenazas por firma**

Gráfica 43. Top 10 amenazas NGFW CAN - junio 2016

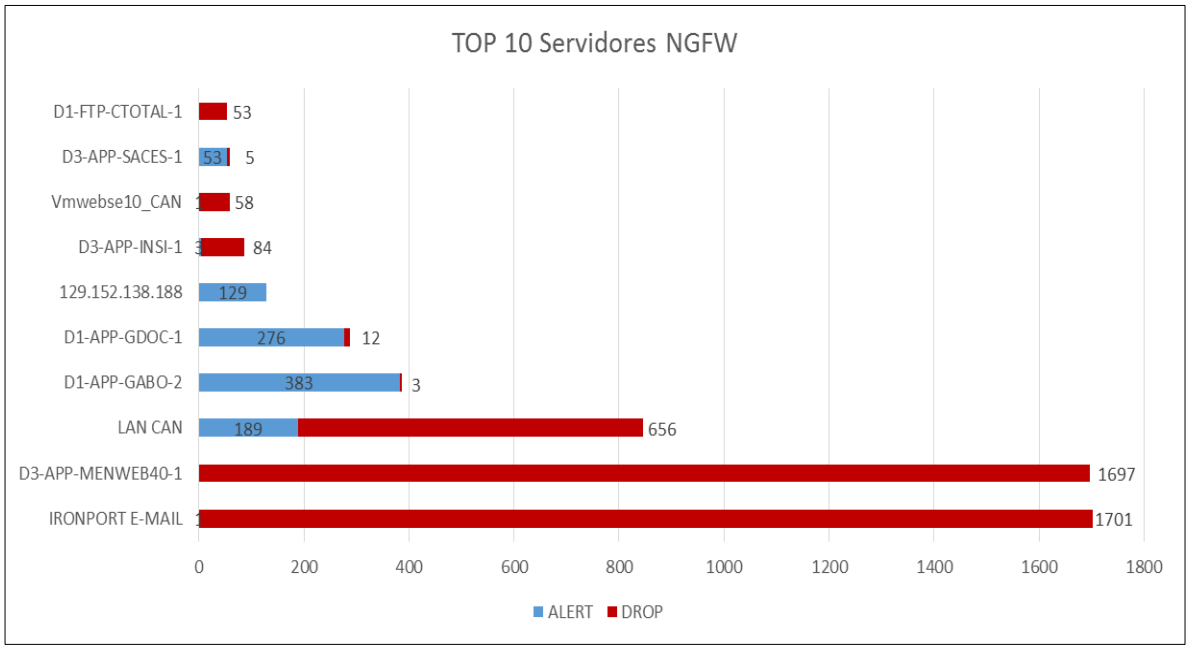


Fuente: Logs NGFW CAN mes de junio 2016.

Como se observa en la gráfica 43, las 3 firmas con mayor número de eventos son: "*Apache Tomcat Windows Installer Default Account Access Vulnerability (34160), Microsoft Outlook Attachment Name Verify Remote Code Execution Vulnerability (34215) y HTTP Request Brute Force Attack (40059),* con el 30.4%, 29.3% y 11.3% respectivamente del total de eventos detectados, donde las barras azules representan los eventos permitidos y las barras de color rojo los eventos bloqueados catalogados como amenazas.

➢ **Top de servidores con más eventos**

Gráfica 44. Top servidores con más eventos NGFW CAN - junio 2016

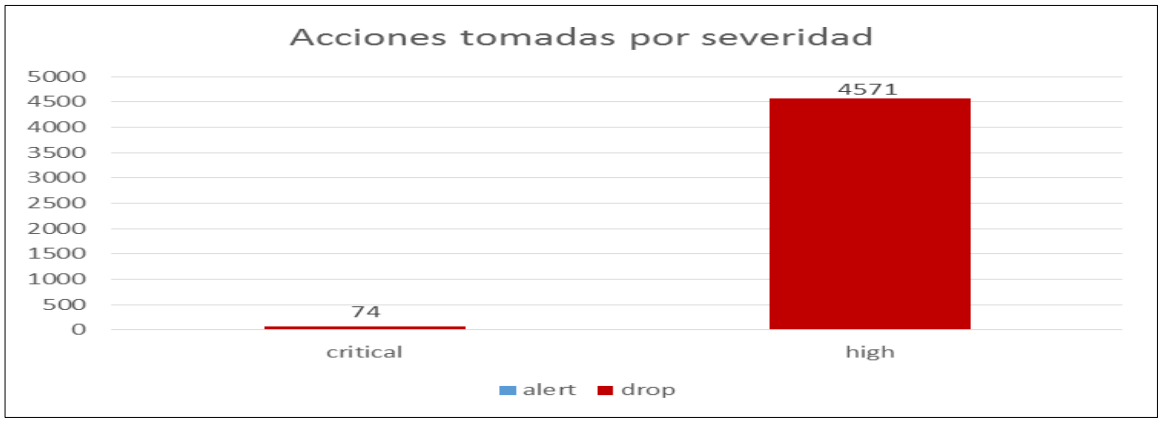


Fuente: Logs NGFW CAN mes de junio 2016.

Como se observa en la gráfica 44, los 3 servidores con mayor número de eventos son: *"IRONPORT E-MAIL"* con el 29.4%, *"D3-APP-MENWEB40-1"* con el 29.3%, y *"LAN CAN"* con el 14.6% del total de eventos detectados, donde las barras azules representan las firmas permitidas y las barras de color rojo las firmas bloqueadas identificadas como amenazas.

- **Acciones por severidad *critical* y *high***

Gráfica 45. Acciones tomadas por severidad NGFW CAN - junio 2016



Fuente: Logs NGFW CAN mes de junio 2016.

Como se observa en la gráfica 45, el 100% de las amenazas con severidades *critical* y *high* están siendo bloqueadas en el NGFW de la sede del CAN.

- **Anti-Virus**

Cuadro 13. Eventos de anti-virus registrado en l el NGFW CAN – junio 2016

Firma virus	Eventos
Virus/Win32.WGeneric.jdxlr (1272639)	15
Worm/Win32.allaple.rgiym (2116762)	13
Worm/Win32.mydoom.prfp (2850026)	13
Virus/Win32.adwind.ax (1252067)	4
Virus/Win32.almanahe.aaws (2043899)	4
Trojan/Win32.menti.dkqk (2278332)	3
Virus/Win32.adwind.aq (1252056)	3
Virus/Win32.adwind.aw (1252066)	3
Virus/Win32.WGeneric.jeztg (2432265)	3
Virus/Win32.slugin.sxg (2332505)	2
Total	**74**[50]

Fuente: Logs NGFW CAN mes de junio 2016.

[50] El total refleja la suma de todos los eventos asociados a las firmas de esta categoría y no solamente los mostrados en el TOP 10.

El 100% de las firmas detectadas por el módulo de anti-virus que se observan en el cuadro 13 fueron bloqueadas.

- **Anti-Spyware**

Cuadro 14. Eventos de anti-spyware registrado en l el NGFW CAN – junio 2016

Firma spyware	Eventos
Sipvicious.Gen User-Agent Traffic (13272)	76655
Suspicious DNS Query (generic:avastzanahoria.no-ip.biz) (4032033)	54750
generic:avastzanahoria.no-ip.biz(3824964)	34273
Xtreme Rat.Gen Command and Control Traffic (13391)	17494
Suspicious DNS Query (generic:ptyisuurwdvi.info) (4016533)	15452
generic:yeockejna.ru(3801022)	15384
generic:kjvfuzapyi.singamount.ru(3825279)	2026
TrojanSpy.nivdort:againstanabolics.com(3811916)	1735
TrojanSpy.nivdort:navstop.ru(3811915)	1732
Morto RDP Request Traffic (13274)	1489
Total	**287125**[51]
Fuente: Logs NGFW CAN mes de junio 2016.	

Las 3 firmas de anti-spyware con mayor número de eventos, de acuerdo al cuadro 14 son: *"Sipvicious.Gen User-Agent Traffic (13272), Suspicious DNS Query (generic: avastzanahoria.no-ip.biz) (4032033) y generic: avastzanahoria.no-ip.biz (3824964)"*, con el 26.7%, 19.1% y 11.9% respectivamente del total de spyware detectado.

El 72.7% de eventos detectados dentro de esta categoría fueron bloqueados luego de que se bloqueara las firmas con severidades *critical, high y medium*, por el incremento progresivo observado de correos maliciosos recibidos en la sede del CAN.

[51] El total refleja la suma de todos los eventos asociados a las firmas de esta categoría y no solamente los mostrados en el TOP 10.

- **Eventos WildFire**

Cuadro 15. Eventos de Wildfire registrado en l el NGFW CAN – junio 2016

Servidor	Android package file detected (52108)	Windows executable (EXE) (52020)	Total general
IRONPORT	1	11	12
LAN_MEN	-	1	1
Total general	**1**	**12**	**13**
Fuente: Logs NGFW CAN mes de junio 2016.			

Los archivos revisados por el sistema Wildfire, que se observan en el cuadro 15, son objetos con probabilidad de ser maliciosos, que son ejecutados y analizados en un entorno controlado. El sistema Wildfire realiza un diagnóstico, en donde si los archivos recientemente analizados se consideran maliciosos, se genera el reporte y se alimenta el repositorio de Palo Alto.

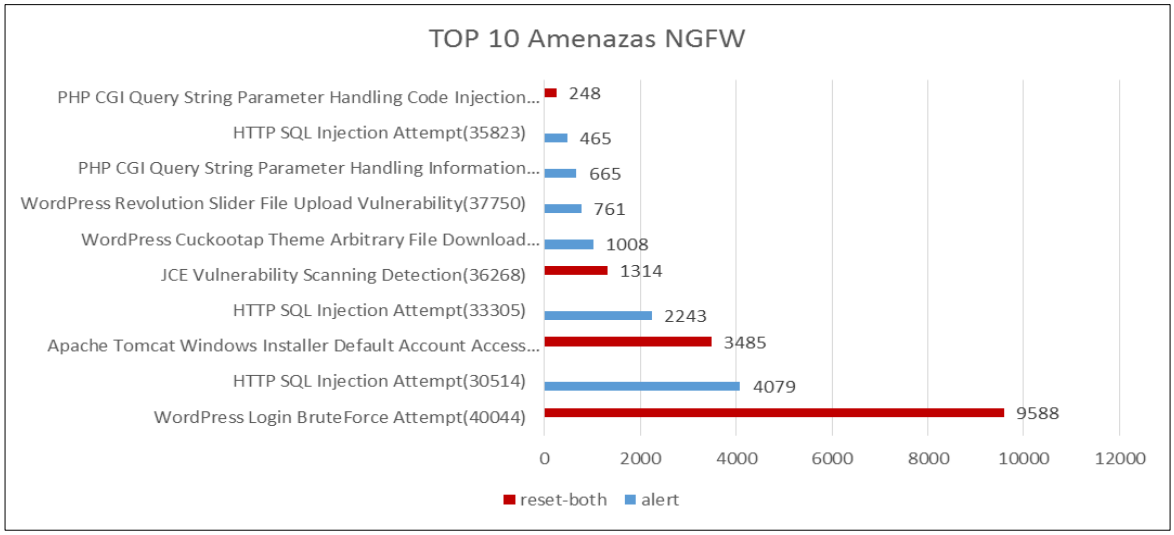
El 92.3% de los eventos diagnosticados por la nube de Palo Alto como "*malware*" o "*grayware*" fueron generados por los usuarios internos del Ministerio (Red LAN). Por tal razón se está promoviendo la política de sitios seguros y el bloqueo de aplicaciones como Tor y otras que buscar saltar el proxy del MEN.

B.3 Reporte mensual estadístico NGFW y WAF – Julio

DIVEO NGFW

- **Top bloqueo por firmas**

Gráfica 46. Top 10 amenazas NGFW DIVEO - julio 2016

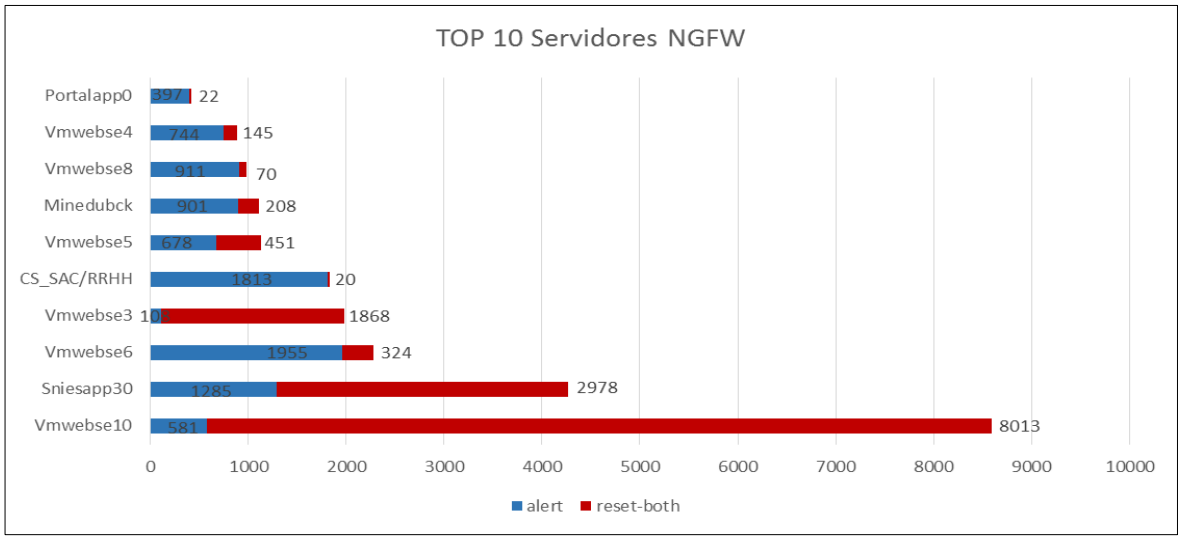


Fuente: Logs NGFW DIVEO mes de julio 2016.

Las 3 firmas con mayor número de eventos de acuerdo a la gráfica 46 identificadas como amenazas son: *"WordPress Login BruteForce Attempt (40044), HTTP SQL Injection Attempt (30514) y Apache Tomcat Windows Installer Default Account Access Vulnerability (34160)"* con el 37.33%, 15.88% y 13.57% respectivamente del total de eventos detectados, donde las barras azules representan los eventos permitidos y las barras de color rojo los eventos bloqueados catalogados como amenazas.

- **Top de servidores con más eventos**

Gráfica 47. Top servidores con más eventos NGFW DIVEO - julio 2016

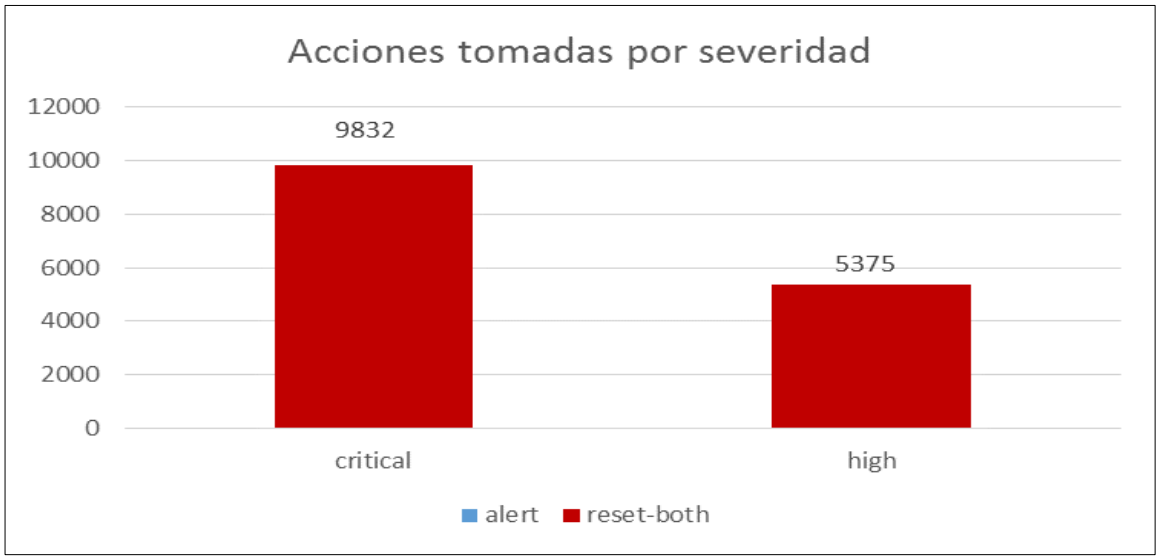


Fuente: Logs NGFW DIVEO mes de julio 2016.

Como se observa en la gráfica 47, los 3 servidores con mayor número de eventos son: *"Vmwebse10"* con el 33.5%, *"Sniesapp30"* con el 16.6% *y "Vmwebse6"* con el 8.9% del total de eventos detectados, donde las barras azules representan las firmas permitidas y las barras de color rojo las firmas bloqueadas identificadas como amenazas.

- **Acciones por severidad *critical* y *high***

Gráfica 48. Acciones tomadas por severidad NGFW DIVEO - julio 2016



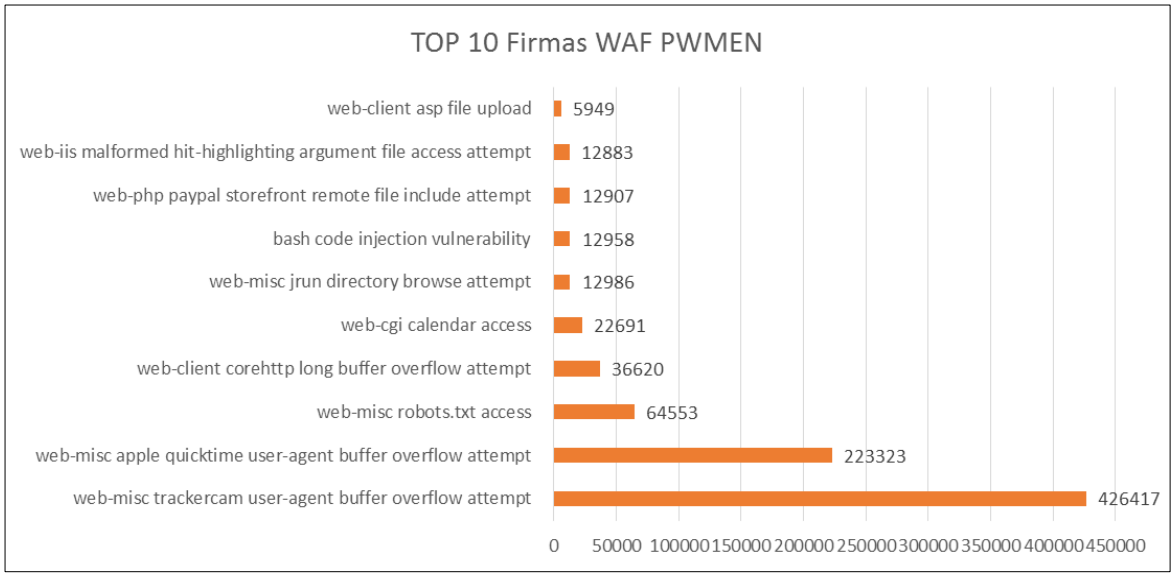
Fuente: Logs NGFW DIVEO mes de julio 2016.

Como se observa en la gráfica 48, el 100% de las amenazas con severidades *critical* y *high* están siendo bloqueadas en el NGFW de la sede de DIVEO.

DIVEO WAF

- **Top amenazas por firmas**

Gráfica 49. Top 10 firmas WAF - julio 2016

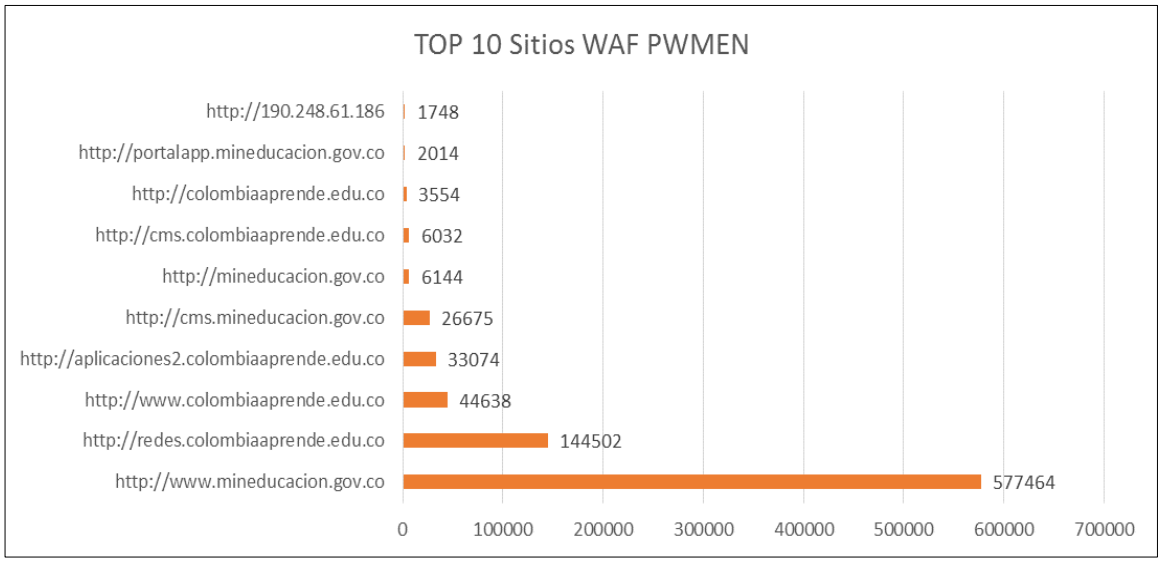


Fuente: Logs WAF mes de julio 2016.

Como se observa en la gráfica 49, las 3 firmas con mayor número de eventos son: *"web-misc trackercam user-agent buffer overflow attempt, web-misc apple quicktime user-agent buffer overflow attempt y web-misc robots.txt access",* con el 49.9%, 26.13% y 7.55% respectivamente del total de eventos presentados.

- **Top sitios web con más eventos**

Gráfica 50. Top 10 sitios WAF - julio 2016

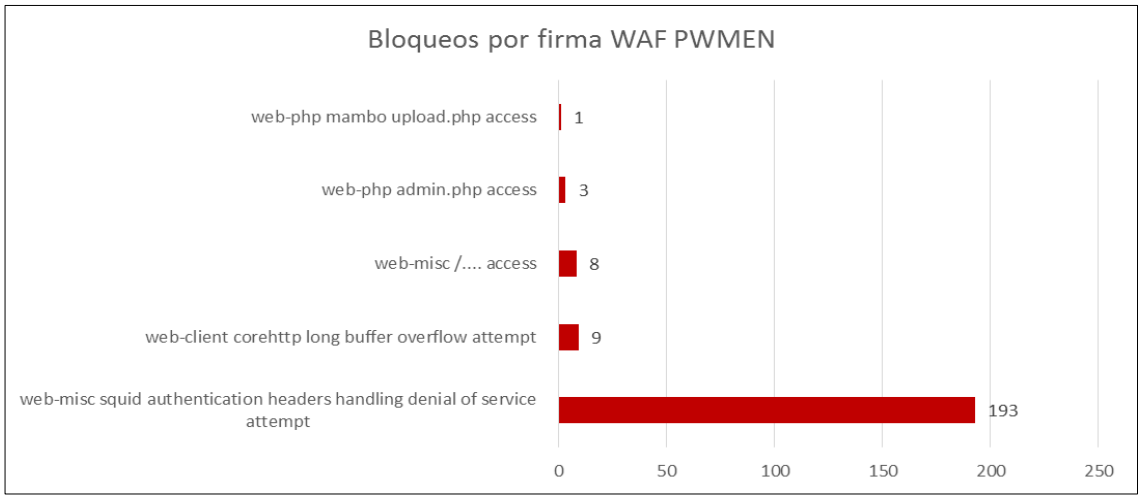


Fuente: Logs WAF mes de julio 2016.

Los 3 sitios web con mayor número de eventos, de acuerdo a la gráfica 50 son: "*www.mineducacion.gov.co"* con el 67.57%, *"redes.colombiaaprende.edu.co"* con el 16.91%, *y "www.colombiaaprende.edu.co"* con el 5.22% del total de eventos presentados.

- **Top bloqueo por firmas**

Gráfica 51. Bloqueo por firmas WAF – julio 2016

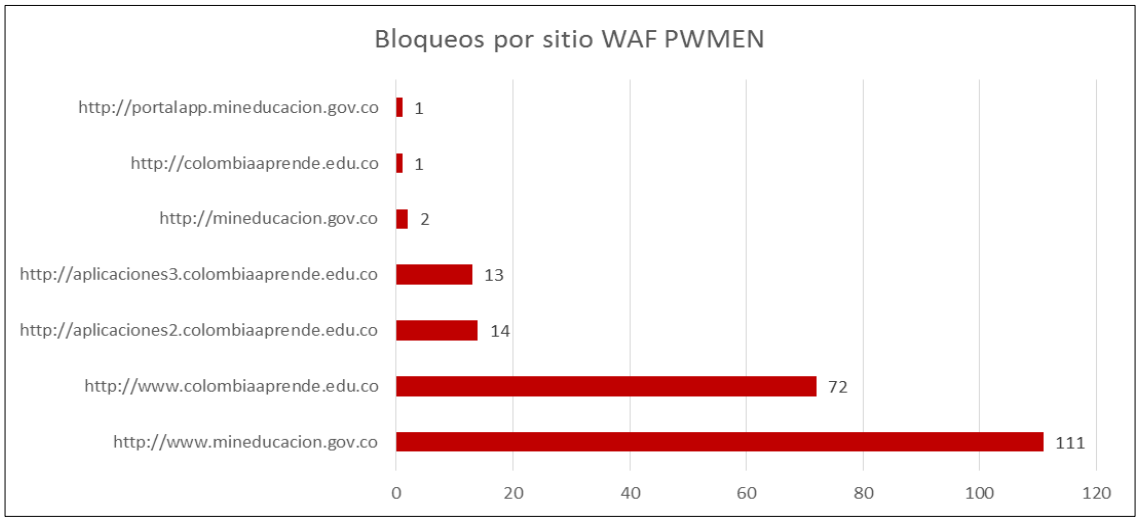


Fuente: Logs WAF mes de julio 2016.

Las 3 firmas con mayor número de bloqueos de acuerdo a la gráfica 51 son: *"web-mis squid authentications headers handing denial of service attemmpt, web-client corehttp long buffer overflow attempr y web-misc/Access"* con un 90%, 4% y 3,7% respectivamente del total de eventos presentados.

- **Top bloqueo por sitios**

Gráfica 52. Bloqueo por sitio WAF – julio 2016



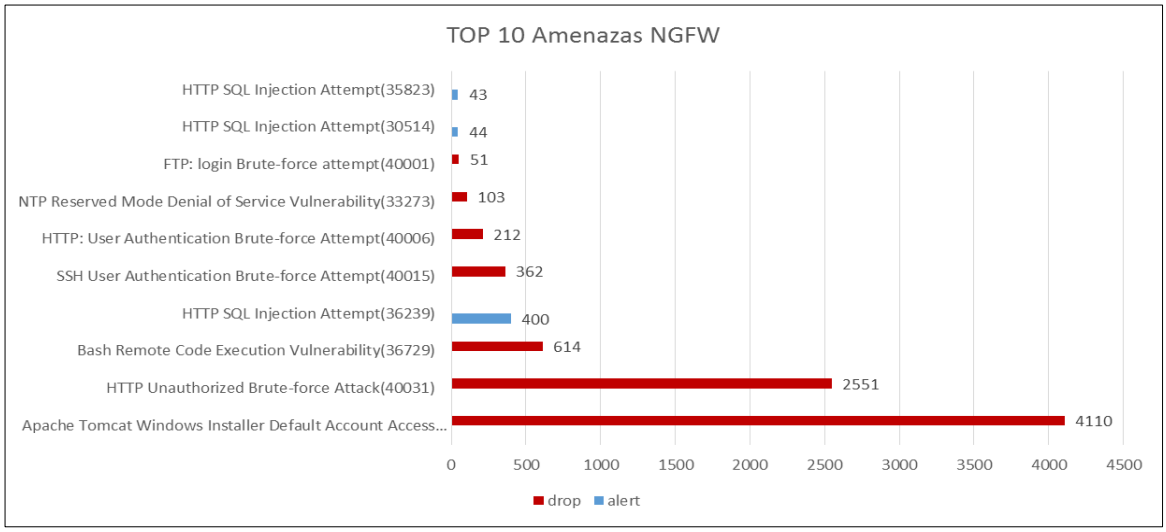
Fuente: Logs WAF mes de julio 2016.

Los 3 sitios web con mayor número de firmas bloqueadas identificadas como amenazas de acuerdo a la gráfica 52 son: *"www.mineducacion.gov.co"*, *"www.colombiaaprende.edu.co"* y *"aplicaciones2.colombiaaprende.edu.co"* correspondiente al 52%, 33,6% y 6,5% respectivamente del total de firmas bloqueadas.

CAN NGFW

- **Top de amenazas por firma**

Gráfica 53. Top 10 amenazas NGFW CAN - julio 2016

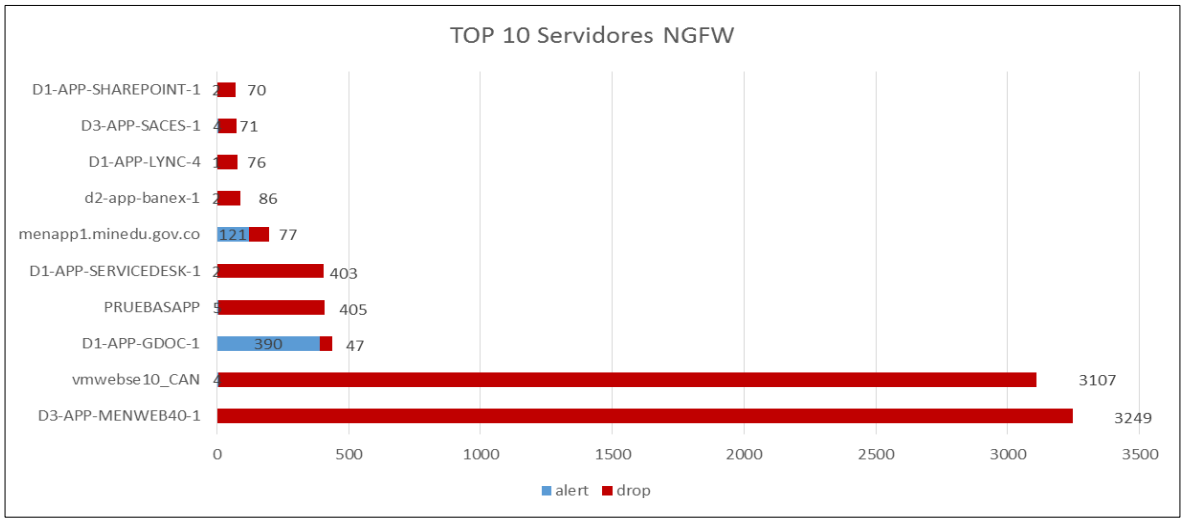


Fuente: Logs NGFW CAN mes de julio 2016.

Como se observa en la gráfica 53, las 3 firmas con mayor número de eventos son: "*Apache Tomcat Windows Installer Default Account Access Vulnerability (34160), HTTP Unauthorized Brute-force Attack (40031) y Bash Remote Code Execution Vulnerability (36729),* acumulando el 46.74%, 29.01% y 6.98% respectivamente del total de eventos detectados, donde las barras azules representan los eventos permitidos y las barras de color rojo los eventos bloqueados catalogados como amenazas.

➢ Top de servidores con más eventos

Gráfica 54. Top servidores con más eventos NGFW CAN - julio 2016

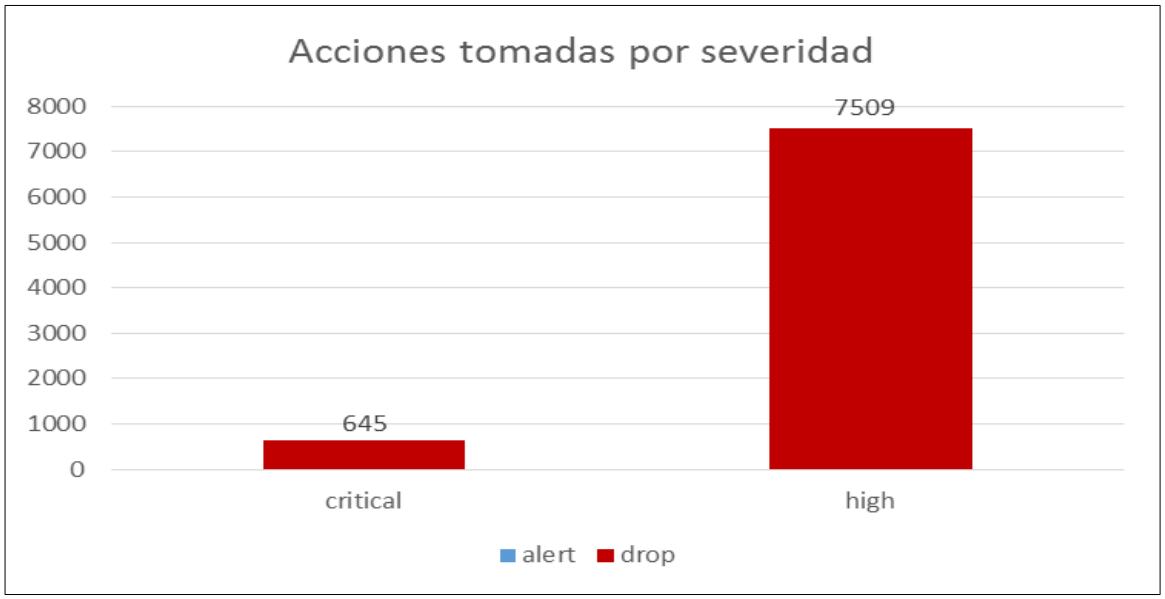


Fuente: Logs NGFW CAN mes de julio 2016.

Como se observa en la gráfica 54, los 3 servidores con mayor número de eventos son: *"D3-APP-MENWEB40-1"* con el 36.9%, *"vmwebse10_CAN"* con el 35.4%, y *"D1-APP-GDOC-1"* con el 4.9% del total de eventos detectados, donde las barras azules representan las firmas permitidas y las barras de color rojo las firmas bloqueadas identificadas como amenazas.

- **Acciones por severidad *critical* y *high***

Gráfica 55. Acciones tomadas por severidad NGFW CAN - julio 2016



Fuente: Logs NGFW CAN mes de julio 2016.

Como se observa en la gráfica 55, el 100% de las amenazas con severidades *critical* y *high* están siendo bloqueadas en el NGFW de la sede del CAN.

- **Anti-Virus**

Cuadro 16. Eventos de anti-virus registrado en l el NGFW CAN – julio 2016

Firma virus	Eventos
Virus/Win32.Adwind.af (1251891)	18
Trojan-SPY/Win32.zbot.ytig (2019191)	4
Worm/Win32.Allaple.aztp (2054763)	3
1252066(1252066)	2
1252067(1252067)	2
Virus/Win32.slugin.tgc (2046389)	2
Virus/Win32.WGeneric.jhgnz (2512786)	2
Virus/Win32.WGeneric.jizch (2433448)	2
Virus/Win32.WGeneric.jjpoh (2220867)	2
Worm/Win32.rebhip.arjo (2432265)	2
Total	**40**[52]
Fuente: Logs NGFW CAN mes de julio 2016.	

El 100% de las firmas detectadas por el módulo de anti-virus que se observan en el cuadro 16 fueron bloqueadas.

[52] El total refleja la suma de todos los eventos asociados a las firmas de esta categoría y no solamente los mostrados en el TOP 10.

- **Anti-Spyware**

Cuadro 17. Eventos de anti-spyware registrado en l el NGFW CAN – julio 2016

Firma spyware	Eventos
Sipvicious.Gen User-Agent Traffic (13272)	63126
Xtreme Rat.Gen Command and Control Traffic (13391)	7973
generic:e0elbkhh9.2nmzh7wrf.com(3805415)	2864
Suspicious DNS Query (generic:00n70r.aingo.cc) (4028643)	2787
Suspicious DNS Query (generic:829lmh.www5.wownthing.cc) (4032033)	1597
Suspicious DNS Query (generic:onichen.ru) (4015521)	1370
SoftwareBundler.dlhelper:pushytype.ru(3824964)	1181
generic:rt.7qg17931793gmy317.com(3823298)	775
Suspicious DNS Query (generic:86igh8koncd5.ahthuvuz.cc) (4066525)	277
generic:ww2.newsystemshield.net(3811916)	243
Total	**90637**[53]
Fuente: Logs NGFW CAN mes de julio 2016.	

Las 3 firmas de anti-spyware con mayor número de eventos, de acuerdo al cuadro 17 son: *"Sipvicious.Gen User-Agent Traffic (13272), Xtreme Rat.Gen Command and Control Traffic (13391) y generic:e0elbkhh9.2nmzh7wrf.com (3805415)*", con el 69.6%, 8.8% y 3.1% respectivamente del total de spyware detectado.

El 30.3% de eventos detectados dentro de esta categoría fueron bloqueados luego de que se aplicara la política de bloqueo de firmas con severidades *critical*, *high* y *medium* por el incremento progresivo de eventos de correos maliciosos recibidos en la sede del CAN.

[53] El total refleja la suma de todos los eventos asociados a las firmas de esta categoría y no solamente los mostrados en el TOP 10.

- **Eventos WildFire**

Cuadro 18. Eventos de Wildfire registrado en l el NGFW CAN – julio 2016.

Servidor	Adobe shockwave flash File (52145)	Microsoft office 2007 word document (52140)	Microsoft PE file (52060)	Windows executable (EXE) (52020)	Total general
IRONPORT EMAIL	-	38	1	412	452
LAN_MEN	-	-	-	10	10
LAN_COMUNICACIONES	1	-	-	-	1
Total general	1	38	1	422	463
Fuente: Logs NGFW CAN mes de julio 2016.					

Los archivos revisados por el sistema Wildfire, que se observan en el cuadro 18, son objetos con probabilidad de ser maliciosos, que son ejecutados y analizados en un entorno controlado. El sistema Wildfire realiza un diagnóstico, en donde si los archivos recientemente analizados se consideran maliciosos, se genera el reporte y se alimenta el repositorio de Palo Alto.

El 97.6% de los eventos diagnosticados por la nube de Palo Alto como "*malware*" o "*grayware*" fueron generados por correos electrónicos que tenían archivos adjuntos con contenido malicioso. Además de las firmas de wildfire-virus que genera el sistema Wildfire de Palo Alto, se generaron políticas de bloqueo para los dominios y asuntos comunes de estos correos en el IronPort E-mail.

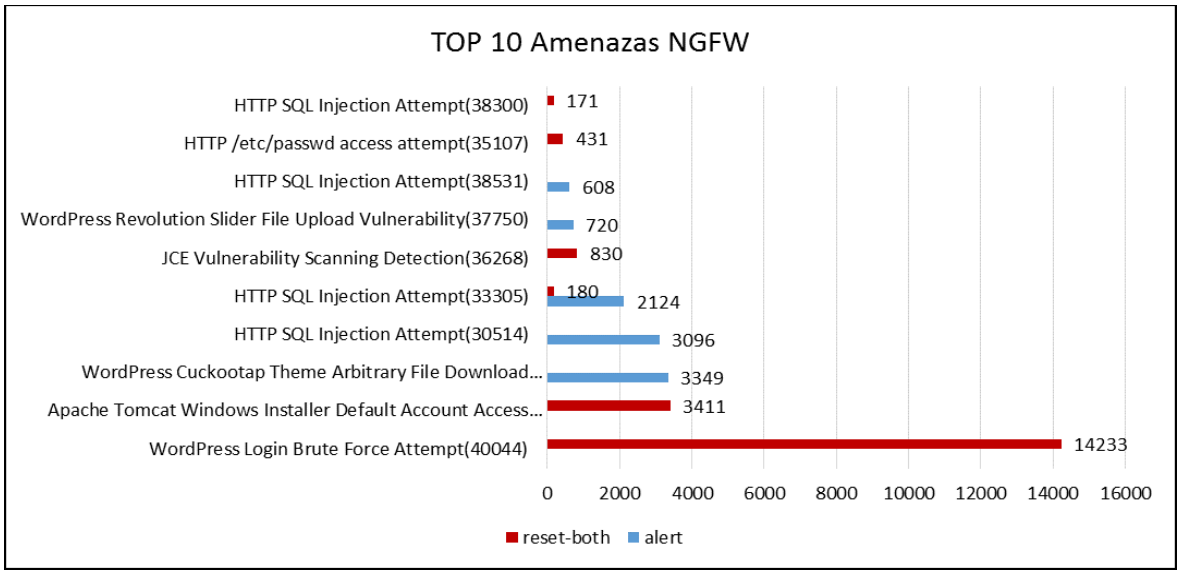
La dirección IP pública 185.83.48.20 generó el 53.7% de eventos de *malware* por SMTP. Se observó que esta IP enviaba correos electrónicos al dominio del Ministerio con asuntos "Aviso importante Factura registrada código seembr512023698741, Factura 963201470001532630010184933654023398971205025105540510 5". El sistema Wildfire generó la firma de virus Virus/Win32.WGeneric.jkagt con ID 3098153 y actualmente bloquea esta variante de virus. La IP está dentro de listas negras por cuanto se recomienda que sea bloqueada de manera preventiva.

C.4 Reporte mensual estadístico NGFW y WAF – Agosto

DIVEO NGFW

- **Top de amenazas por firma**

Gráfica 56. Top 10 amenazas NGFW DIVEO - agosto 2016



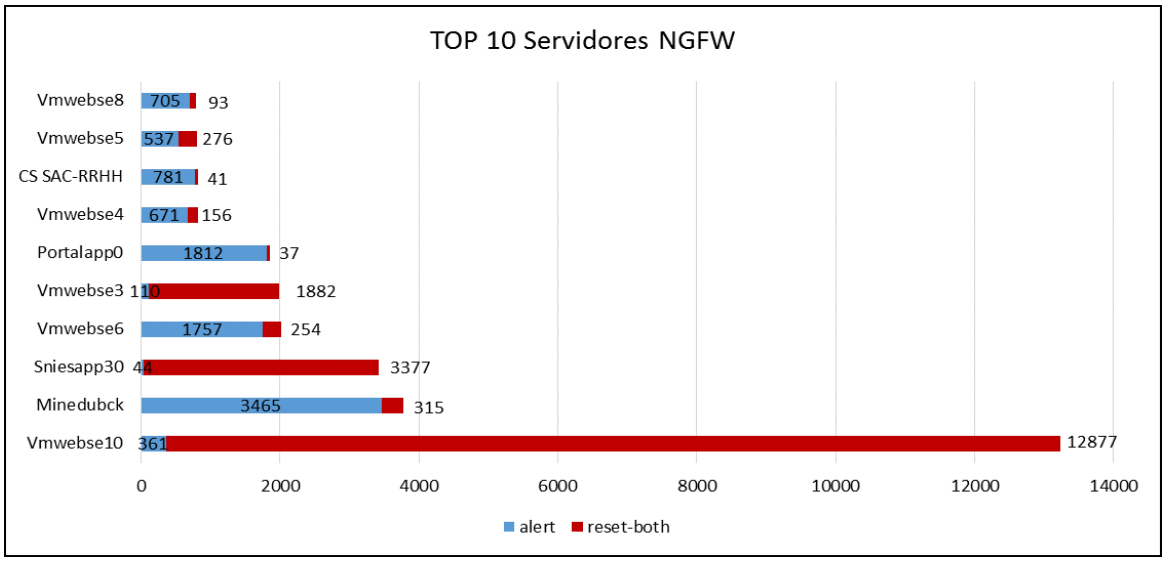
Fuente: Logs NGFW DIVEO mes de agosto 2016.

Como se observa en la gráfica 56, las 3 firmas con mayor número de eventos son: *"WordPress Login BruteForce Attempt (40044), Apache Tomcat Windows Installer Default Account Access Vulnerability (34160) y WordPress Cuckootap Theme Arbitrary File Download Vulnerability (37363)", acumulando* el 45.9%, 11% y 10.8% respectivamente del total de eventos detectados, donde las barras azules representan los eventos permitidos y las barras de color rojo los eventos bloqueados catalogados como amenazas.

Luego de aplicar el bloqueo de la firma "*HTTP SQL Injection Attempt (33305)*", se observan 180 eventos bloqueados para el mes de agosto.

- **Top de servidores con más eventos**

Gráfica 57. Top servidores con más eventos NGFW DIVEO - agosto 2016

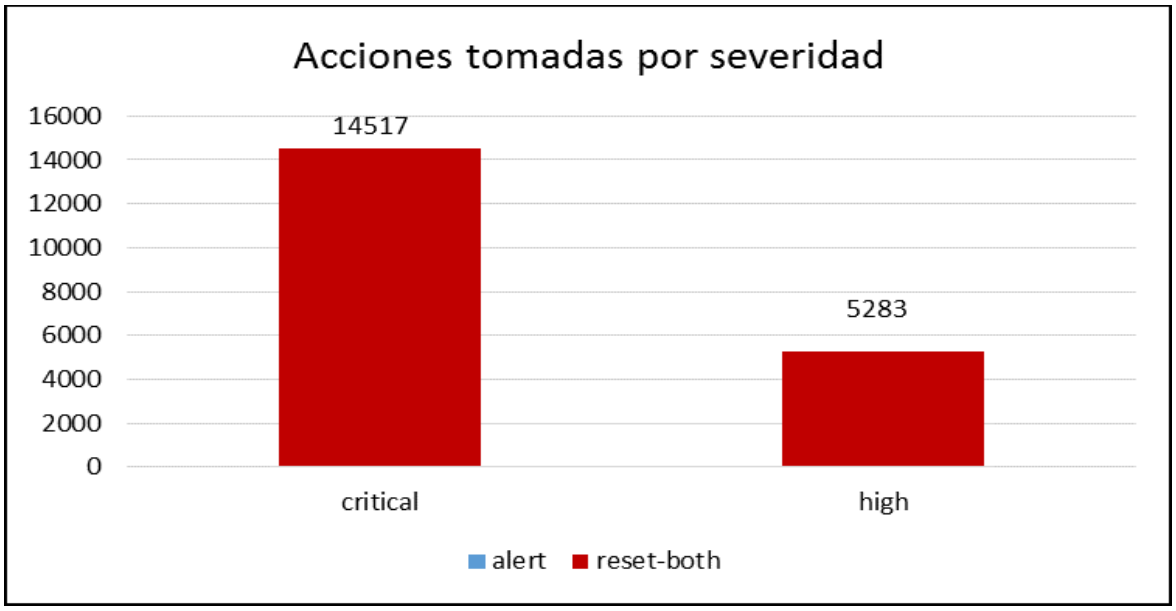


Fuente: Logs NGFW DIVEO mes de agosto 2016.

Como se observa en la gráfica 57, los 3 servidores con mayor número de eventos son: *"Vmwebse10"* con el 42.7%, *"Minedubck"* con el 12.2% *y "Sniesapp30"* con el 11% del total de eventos detectados, donde las barras azules representan las firmas permitidas y las barras de color rojo las firmas bloqueadas identificadas como amenazas.

- **Acciones por severidad *critical* y *high***

Gráfica 58. Acciones tomadas por severidad NGFW DIVEO - agosto 2016



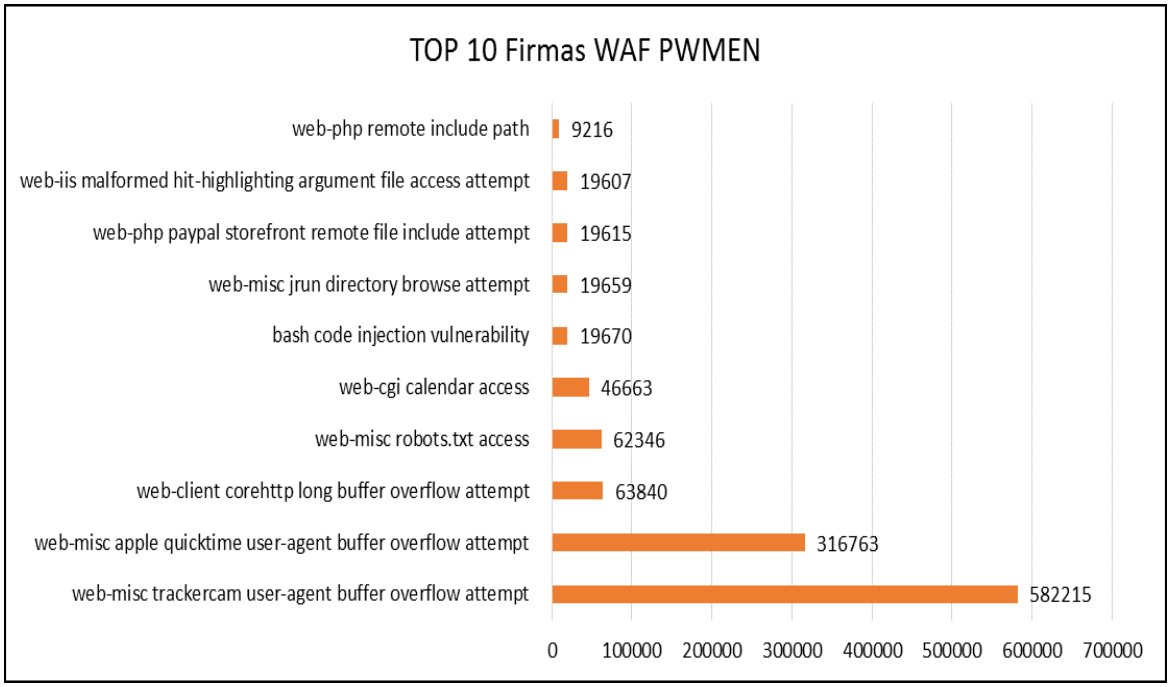
Fuente: Logs NGFW DIVEO mes de agosto 2016.

Como se observa en la gráfica 58, el 100% de las amenazas con severidades *critical* y *high*, están siendo bloqueadas en el NGFW de la sede de DIVEO.

DIVEO WAF

- **Top amenazas por firmas**

Gráfica 59. Top 10 firmas WAF - agosto 2016

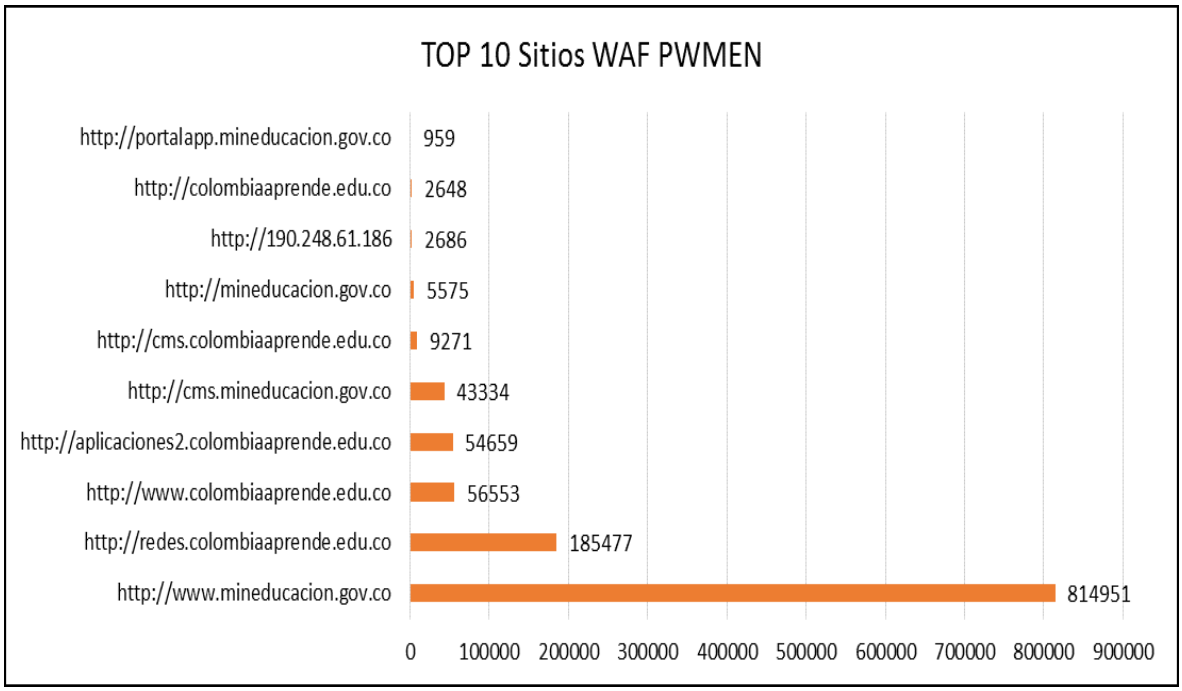


Fuente: Logs WAF mes de agosto 2016.

Como se observa en la gráfica 59, las 3 firmas con mayor número de eventos son: *"web-misc trackercam user-agent buffer overflow attempt, web-misc apple quicktime user-agent buffer overflow attempt y web-client corehttp long buffer overflow attempt",* con el 49.25%, 26.8% y 5.4% respectivamente del total de eventos presentados.

- **Top sitios web con más eventos**

Gráfica 60. Top 10 sitios WAF - agosto 2016

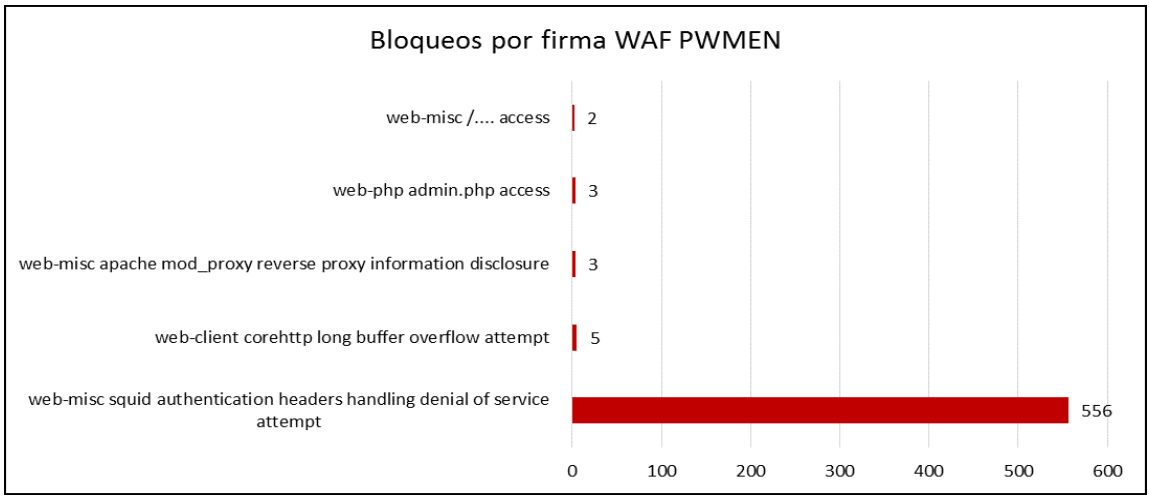


Fuente: Logs WAF mes de agosto 2016.

Los 3 sitios web con mayor número de eventos, de acuerdo a la gráfica 60 son: *"www.mineducacion.gov.co"* con el 68.9%, *"redes.colombiaaprende.edu.co"* con el 15.69%, *y "www.colombiaaprende.edu.co"* con el 4.8% del total de eventos presentados.

- **Top bloqueo por firmas**

Gráfica 61. Bloqueo por firmas WAF – agosto 2016

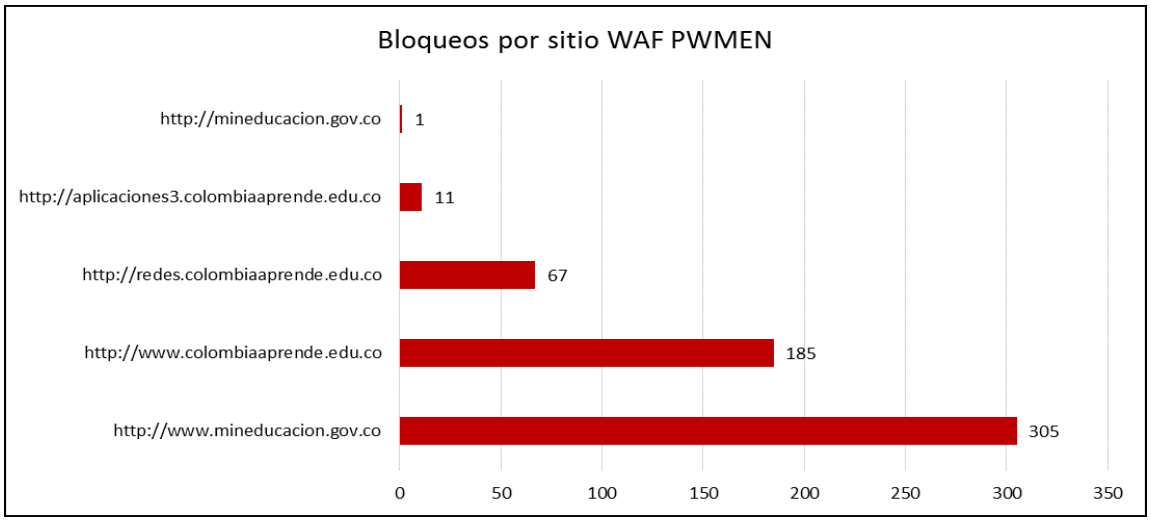


Fuente: Logs WAF mes de agosto 2016.

Las 3 firmas con mayor número de bloqueos de acuerdo a la gráfica 61 identificadas como amenazas son: *"web-mis squid authentications headers handing denial of service attemmpt, web-misc/Access y web-mis apache mod_proxy reverse information disclousure"* con un 89%, 4% y 3,5% respectivamente del total de eventos presentados.

- **Top bloqueo por sitios**

Gráfica 62. Bloqueo por sitio WAF – agosto 2016



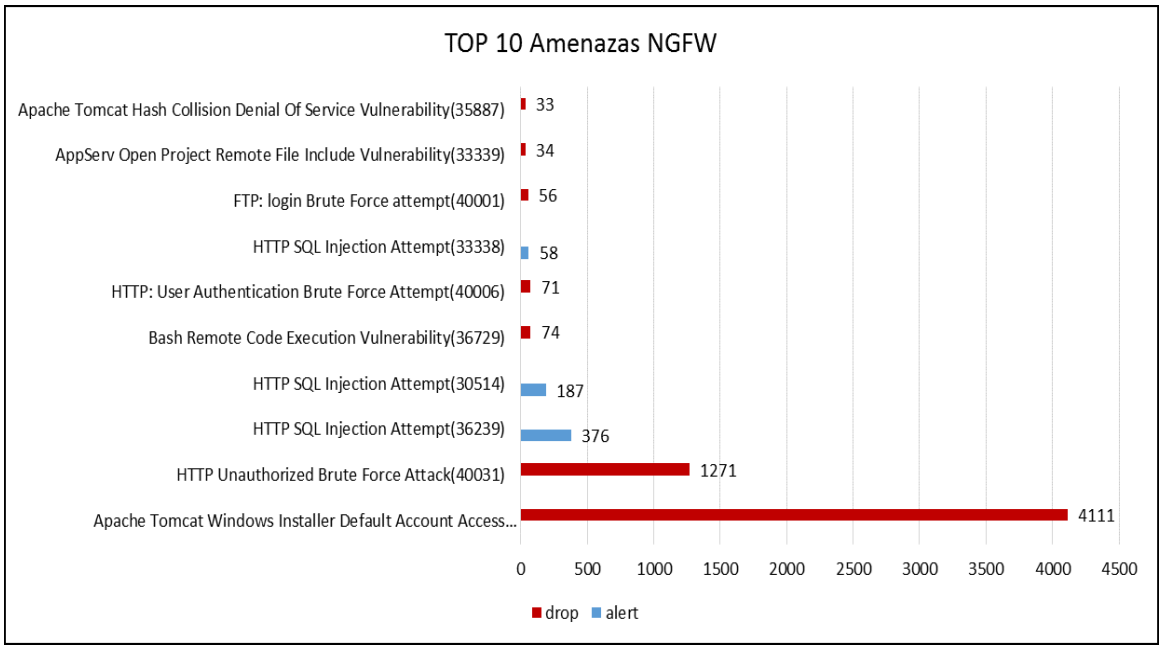
Fuente: Logs WAF mes de agosto 2016.

Los 3 sitios web con mayor número de firmas bloqueadas identificadas como amenazas de acuerdo a la gráfica 62 son: *"www.mineducacion.gov.co"*, *"www.colombiaaprende.edu.co"* y *"redes.colombiaaprende.edu.co"* correspondiente al 52%, 33.6% y 6.5% respectivamente del total de firmas bloqueadas.

CAN NGFW

- **Top de amenazas por firma**

Gráfica 63. Top 10 amenazas NGFW CAN - agosto 2016

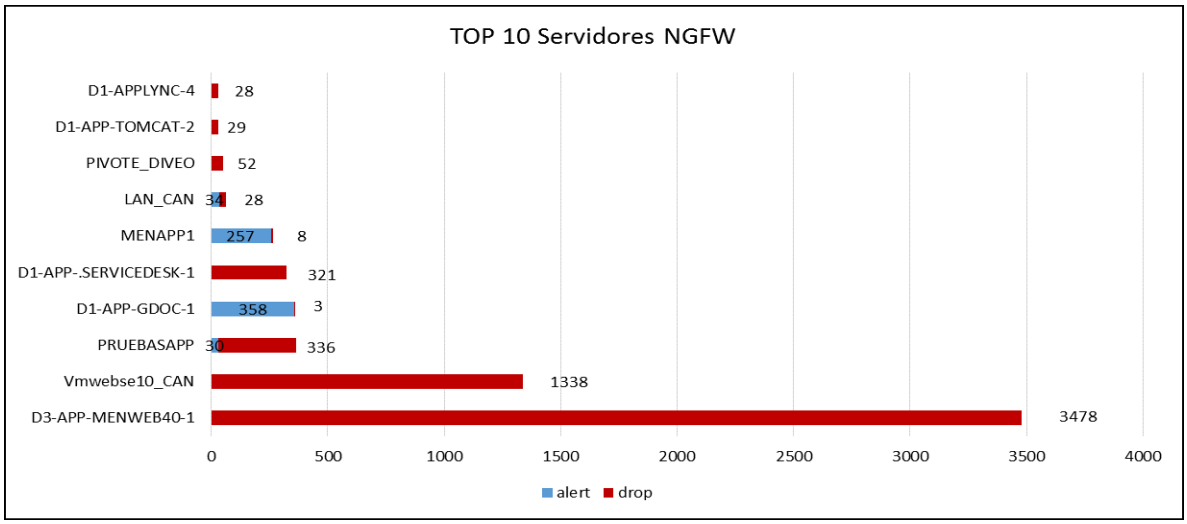


Fuente: Logs NGFW CAN mes de agosto 2016.

Como se observa en la gráfica 63, las 3 firmas con severidades *médium*, *high* y *critical*, con mayor número de eventos son: "*Apache Tomcat Windows Installer Default Account Access Vulnerability (34160), HTTP Unauthorized Brute-force Attack (40031) HTTP SQL Injection Attempt (36239),* acumulando el 63.73%, 19.7% y 5.83% respectivamente del total de eventos detectados, donde las barras azules representan los eventos permitidos y las barras de color rojo los eventos bloqueados catalogados como amenazas.

- **Top de servidores con más eventos**

Gráfica 64. Top servidores con más eventos NGFW DIVEO - agosto 2016

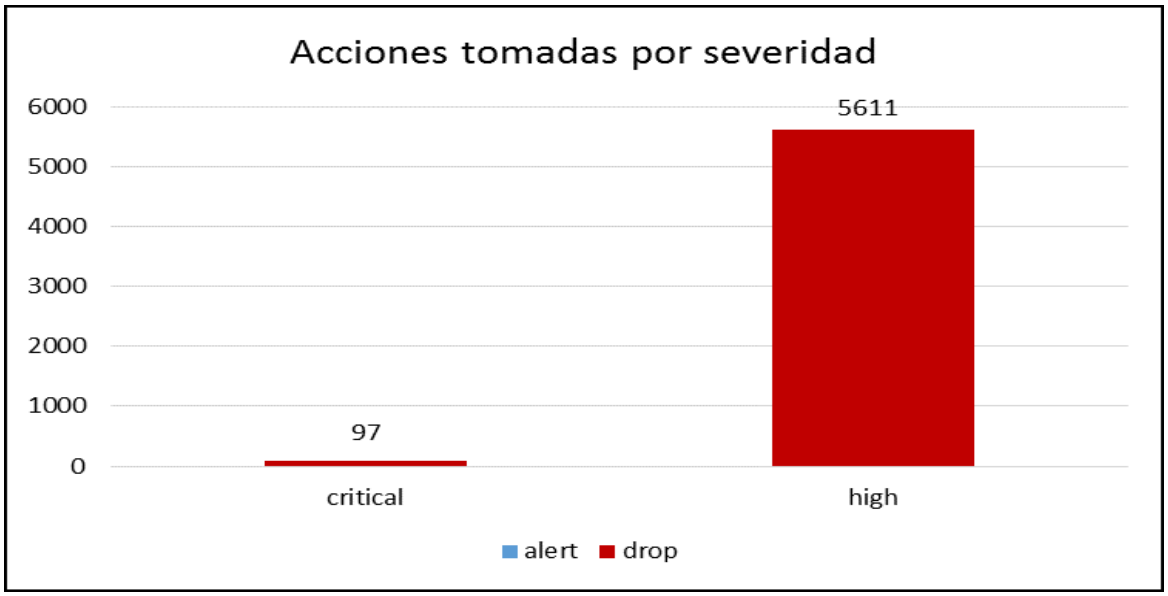


Fuente: Logs NGFW DIVEO mes de agosto 2016.

Como se observa en la gráfica 64, los 3 servidores con mayor número de eventos son: *"D3-APP-MENWEB40-1"* con el 53.9%, *"vmwebse10_CAN"* con el 20.7%, y *"PRUEBASAPP"* con el 5.6% del total de eventos detectados, donde las barras azules representan las firmas permitidas y las barras de color rojo las firmas bloqueadas identificadas como amenazas.

- **Acciones por severidad *critical* y *high***

Gráfica 65. Acciones tomadas por severidad NGFW CAN - agosto 2016



Fuente: Logs NGFW CAN mes de agosto 2016.

Como se observa en la gráfica 65, el 100% de las amenazas con severidades *critical* y *high*, están siendo bloqueadas en el NGFW de la sede del CAN.

- **Anti-Virus**

Cuadro 19. Eventos de anti-virus registrado en l el NGFW CAN – agosto 2016

Firma virus	Eventos
Virus/Win32.Adwind.af (1251891)	6
Virus/Android.WGeneric.jkzyy (1008917)	3
Virus/Win32.slugin.sre (2047976)	3
Trojan/Win32.forucon.amm (2065154)	2
Virus/Win32.WGeneric.hknqi (2037618)	2
Virus/Win32.xorer.jvd (2026847)	2
Backdoor/Win32.kuluoz.bsl (2858554)	1
Virus/Win32.ramnit.azkyv (2659509)	1
Virus/Win32.WGeneric.jecqe (2570059)	1
Virus/Win32.WGeneric.jltmb (2351780)	1
Total	**23**[54]
Fuente: Logs NGFW CAN mes de agosto 2016.	

El 100% de las firmas detectadas por el módulo de anti-virus que se observan en el cuadro 19 fueron bloqueadas.

[54] El total refleja la suma de todos los eventos asociados a las firmas de esta categoría y no solamente los mostrados en el TOP 10.

- **Anti-Spyware**

Cuadro 20. Eventos de anti-spyware registrado en l el NGFW CAN – agosto 2016

Firma spyware	Eventos
Sipvicious.Gen User-Agent Traffic (13272)	126627
Suspicious DNS Query (generic:804891.cc) (4017107)	4539
generic:www.178stu.com(3839158)	3259
Xtreme Rat.Gen Command and Control Traffic (13391)	2524
TrojanSpy.nivdort:cleansportswomen.com(3838437)	226
TrojanSpy.nivdort:againstanabolics.com(3838698)	217
TrojanSpy.nivdort:navstop.ru(3838697)	207
generic:westride.net(3813487)	80
generic:driveslow.net(3813489)	66
generic:fieldpress.net(3812712)	48
Total	**145793**[55]
Fuente: Logs NGFW CAN mes de agosto 2016.	

Las 3 firmas de anti-spyware con mayor número de eventos, de acuerdo al cuadro 20 son: *"Sipvicious.Gen User-Agent Traffic (13272), Suspicious DNS Query (generic: 804891.cc) (4017107) y generic: www.178stu.com (3839158)"*, con el 86.8%, 3.1% y 2.2% respectivamente del total de spyware detectado.

[55] El total refleja la suma de todos los eventos asociados a las firmas de esta categoría y no solamente los mostrados en el TOP 10.

- **Eventos WildFire**

Cuadro 21. Eventos de Wildfire registrado en l el NGFW CAN – agosto 2016.

Servidor	Java class file (52117)	Microsoft MS office (52033)	Microsoft office 2007 word document (52140)	Windows executable (EXE) (52020)	Total general
IRONPORT EMAIL	1	7	71	10	89
LAN_CAN	-	-	-	27	27
COMUNICACIONES	-1	-	-	-	1
Total general	**1**	**7**	**71**	**37**	**117**

Fuente: Logs NGFW CAN mes de agosto 2016.

Los archivos revisados por el sistema Wildfire, que se observan en el cuadro 21, son objetos con probabilidad de ser maliciosos, que son ejecutados y analizados en un entorno controlado. El sistema Wildfire realiza un diagnóstico, en donde si los archivos recientemente analizados se consideran maliciosos, se genera el reporte y se alimenta el repositorio de Palo Alto.

El 76.1% de los eventos diagnosticados por la nube de Palo Alto como "*malware*" o "*grayware*" fueron generados por correos electrónicos que tenían archivos adjuntos con contenido malicioso. Además de las firmas de wildfire-virus que genera el sistema Wildfire de Palo Alto, se generaron políticas de bloqueo para los dominios y asuntos comunes de estos correos en el IronPort E-mail.

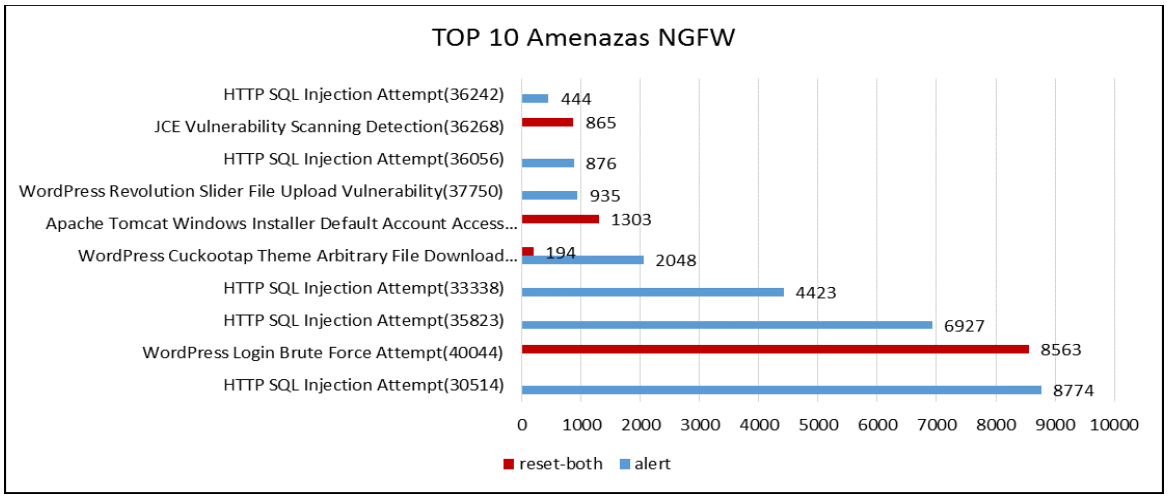
La dirección IP pública 185.83.48.20 generó el 5.1% de eventos de *malware* por SMTP. Se observó que esta IP enviaba correos electrónicos al dominio del Ministerio con asuntos "Aviso importante Factura registrada código seembr512023698741, Factura 963201470001532630010184933654023398971205025105540510 5". El sistema Wildfire generó la firma de virus Virus/Win32.WGeneric.jkagt con ID 3098153 y actualmente bloquea esta variante de virus. La IP está dentro de listas negras por cuanto se recomienda que sea bloqueada de manera preventiva.

C.5 Reporte mensual estadístico NGFW y WAF – Septiembre

DIVEO NGFW

- **Top de amenazas por firma**

Gráfica 66. Top 10 amenazas NGFW DIVEO - septiembre 2016



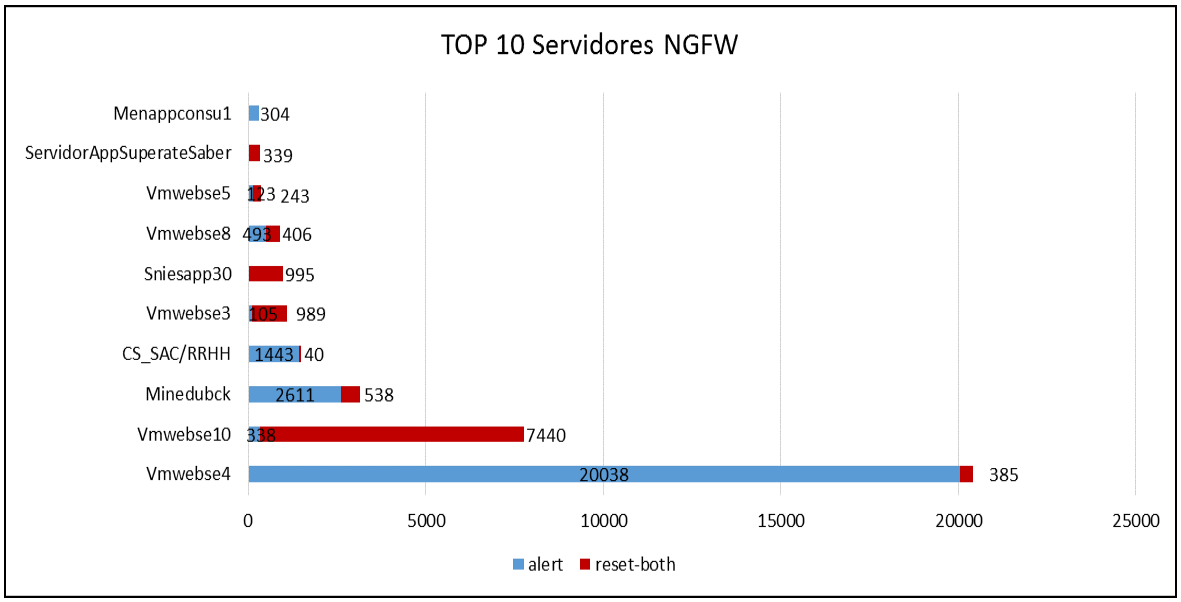
Fuente: Logs NGFW DIVEO mes de septiembre 2016.

Como se observa en la gráfica 66, las 3 firmas con mayor número de eventos son: *"HTTP SQL Injection Attempt (30514), WordPress Login BruteForce Attempt (40044), "HTTP SQL Injection Attempt (35823)",* correspondientemente al 22.8%, 22.3% y 18% respectivamente del total de eventos detectados, donde las barras azules representan los eventos permitidos y las barras de color rojo los eventos bloqueados catalogados como amenazas.

Para este mes se puede observar el bloqueo de la firma denominada "*WordPress Cuckootap Theme Arbitrary File Download Vulnerability (37363)*" con 194 eventos bloqueados.

- **Top de servidores con más eventos**

Gráfica 67. Top servidores con más eventos NGFW DIVEO - septiembre 2016

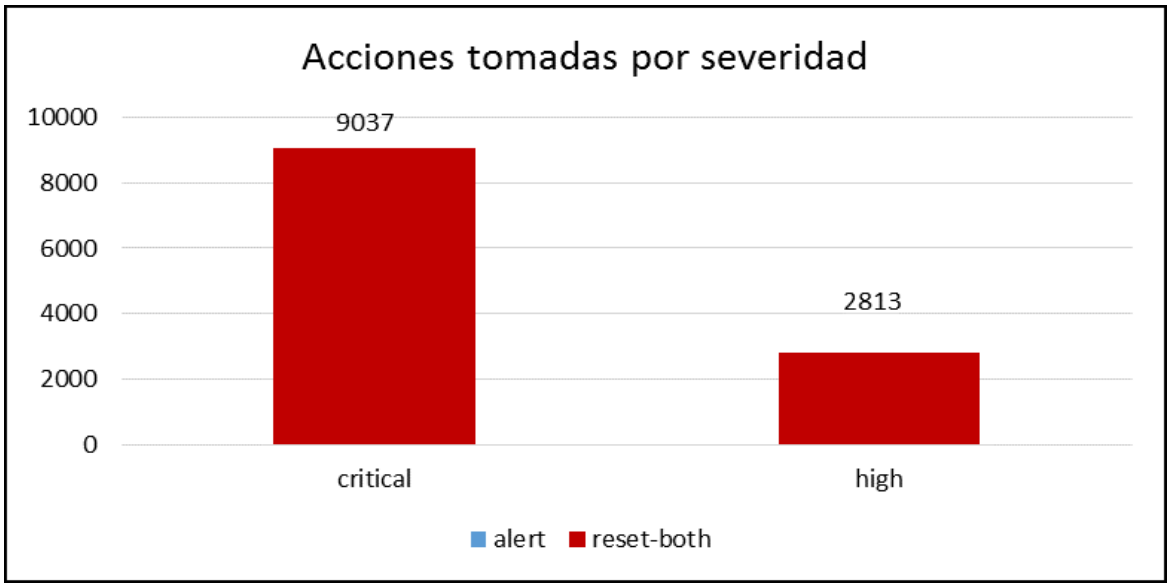


Fuente: Logs NGFW DIVEO mes de septiembre 2016.

Como se observa en la gráfica 67, los 3 servidores con mayor número de eventos son: *"Vmwebse4"* con el 53%, *"Vmwebse10"* con el 20.2% *y "Minedubck"* con el 8.2% del total de eventos detectados, donde las barras azules representan las firmas permitidas y las barras de color rojo las firmas bloqueadas identificadas como amenazas.

- **Acciones por severidad *critical* y *high***

Gráfica 68. Acciones tomadas por severidad NGFW DIVEO - septiembre 2016



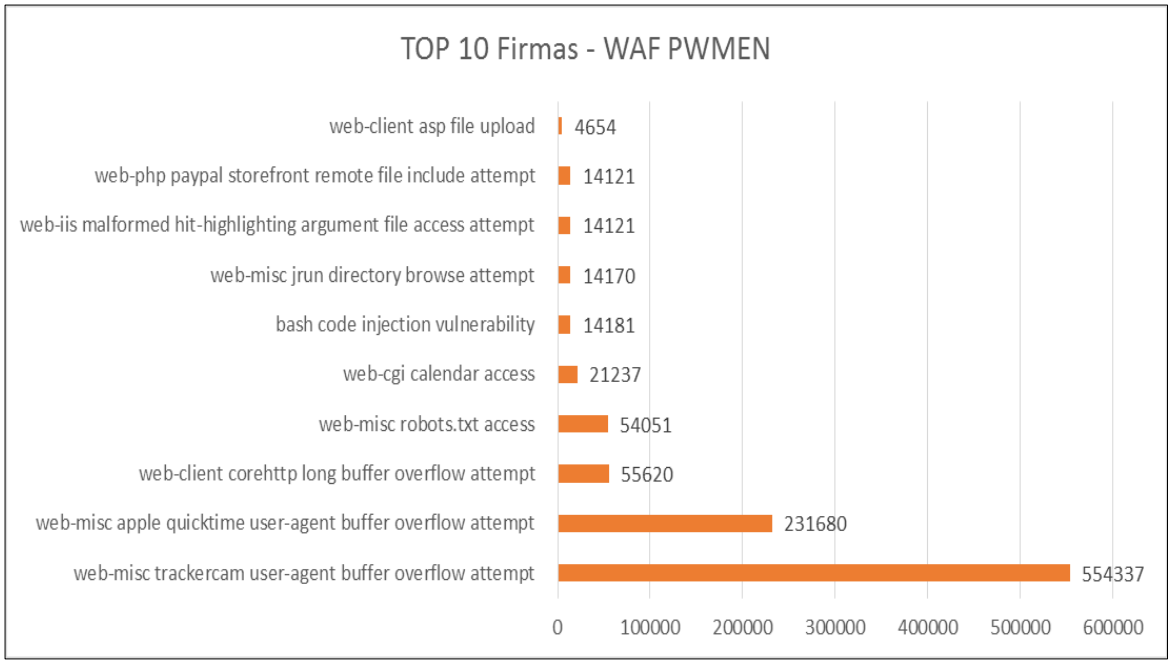
Fuente: Logs NGFW DIVEO mes de septiembre 2016.

Como se observa en la gráfica 68, el 100% de las amenazas con severidades *critical* y *high*, están siendo bloqueadas en el NGFW de la sede de DIVEO.

DIVEO WAF

- **Top amenazas por firmas**

Gráfica 69. Top 10 firmas WAF - septiembre 2016

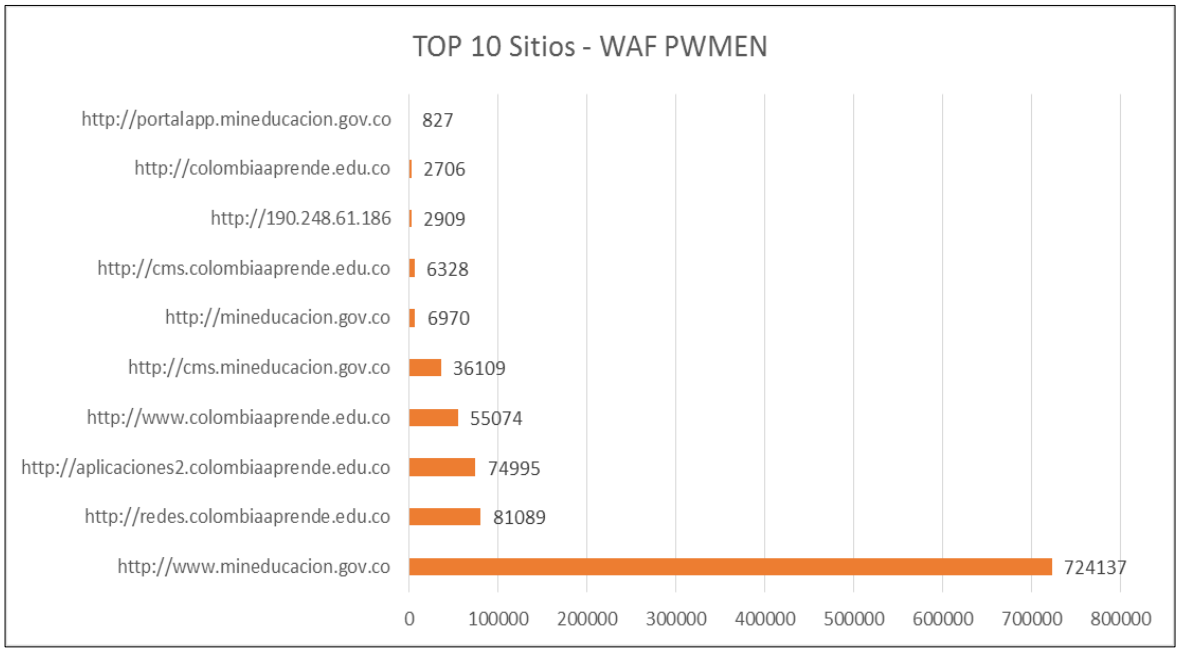


Fuente: Logs WAF mes de septiembre 2016.

Como se observa en la gráfica 69, las 3 firmas con mayor número de eventos son: *web-misc trackercam user-agent buffer overflow attempt, web-misc apple quicktime user-agent buffer overflow attempt y web-client corehttp long buffer overflow attempt",* con el 56%, 23% y 6% respectivamente del total de eventos presentados.

- **Top sitios web con más eventos**

Gráfica 70. Top 10 sitios WAF - septiembre 2016

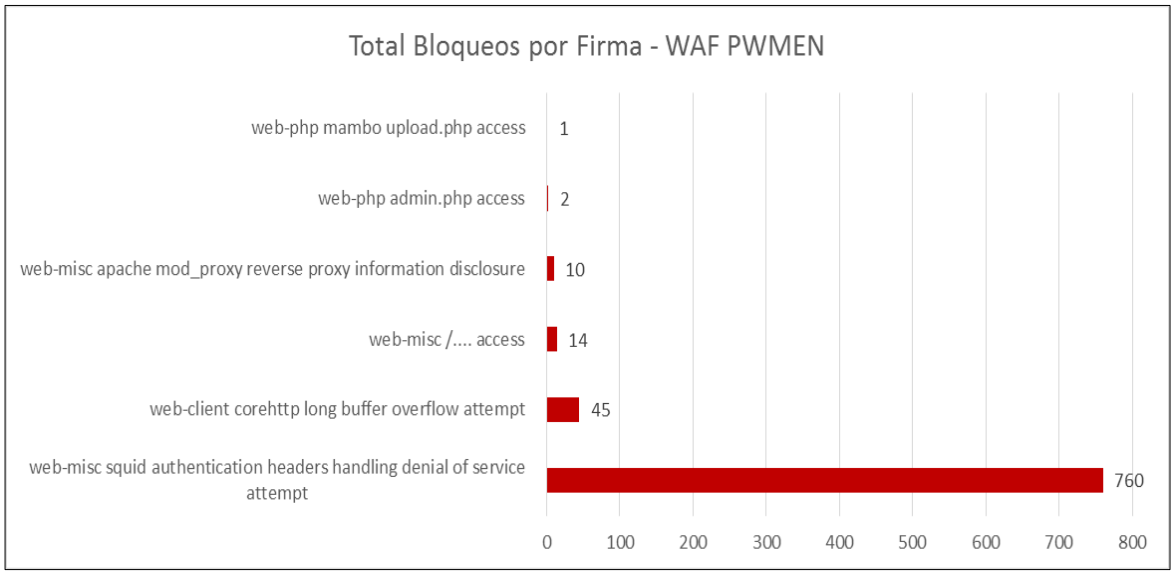


Fuente: Logs WAF mes de septiembre 2016.

Los 3 sitios web con mayor número de eventos, de acuerdo a la gráfica 70 son: *"www.mineducacion.gov.co"* con el 73%, *"redes.colombiaaprende.edu.co"* con el 8%, *y "aplicaciones2.colombiaaprende.edu.co"* con el 8% del total de eventos presentados.

- **Top bloqueo por firmas**

Gráfica 71. Bloqueo por firmas WAF – mayo 2016

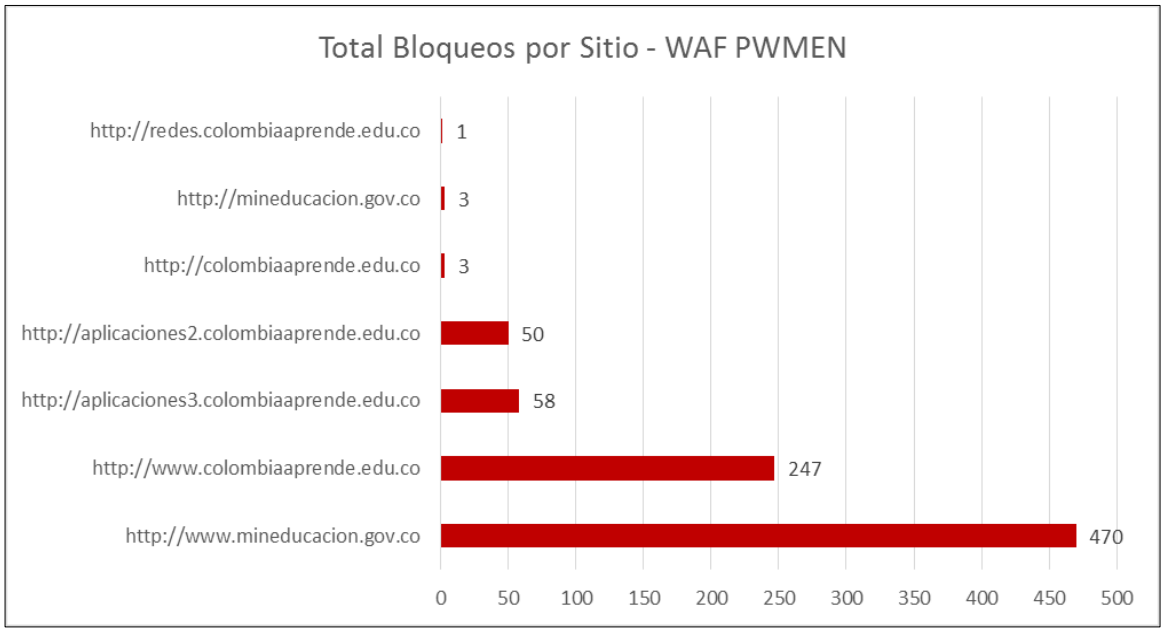


Fuente: Logs WAF mes de septiembre 2016.

Las 3 firmas con mayor número de bloqueos de acuerdo a la gráfica 71 identificadas como amenazas son: *"web-mis squid authentications headers handing denial of service attemmpt, Web-client corehttp long buffer overflow atrempt y web-misc/Access"* con un 91%, 5,4% y 1,8% respectivamente del total de eventos presentados.

- **Top bloqueo por sitios**

Gráfica 72. Bloqueo por sitio WAF – septiembre 2016



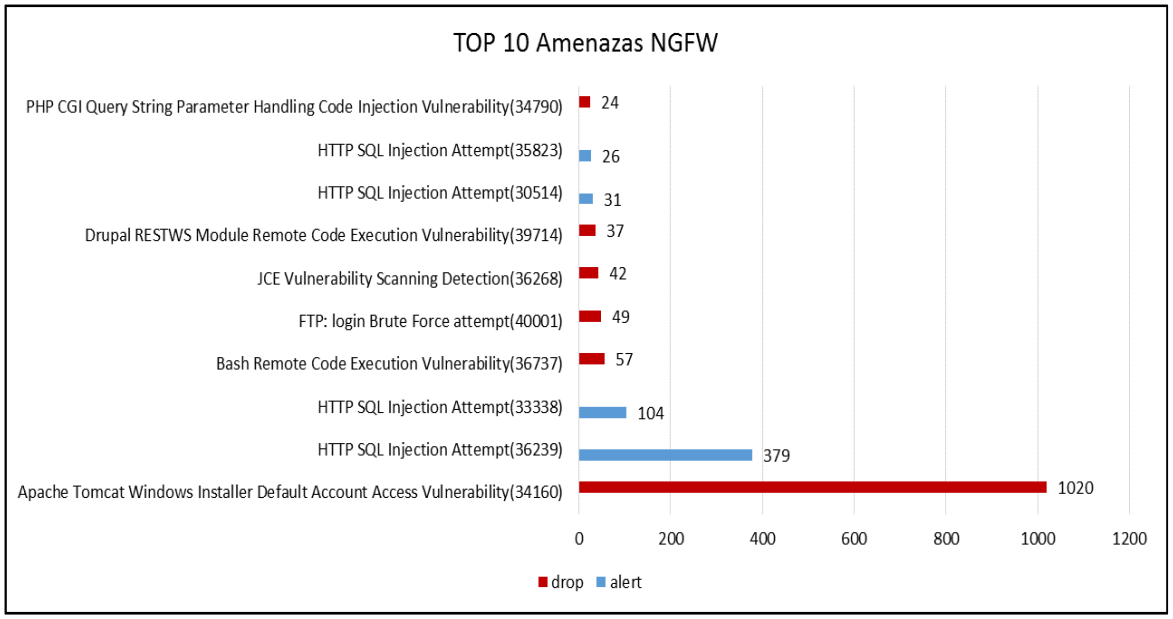
Fuente: Logs WAF mes de septiembre 2016.

Como se observa en la gráfica 72, los 3 sitios web con mayor número de firmas bloqueadas identificadas como amenazas son: *"www.mineducacion.gov.co"* con el 56%, *"www.colombiaaprende.edu.co"* con el 30% y *"aplicaciones3.colombiaaprende.edu.co"* con el 7%, del total de firmas bloqueadas.

CAN NGFW

- **Top de amenazas por firma**

Gráfica 73. Top 10 amenazas NGFW DIVEO - septiembre 2016

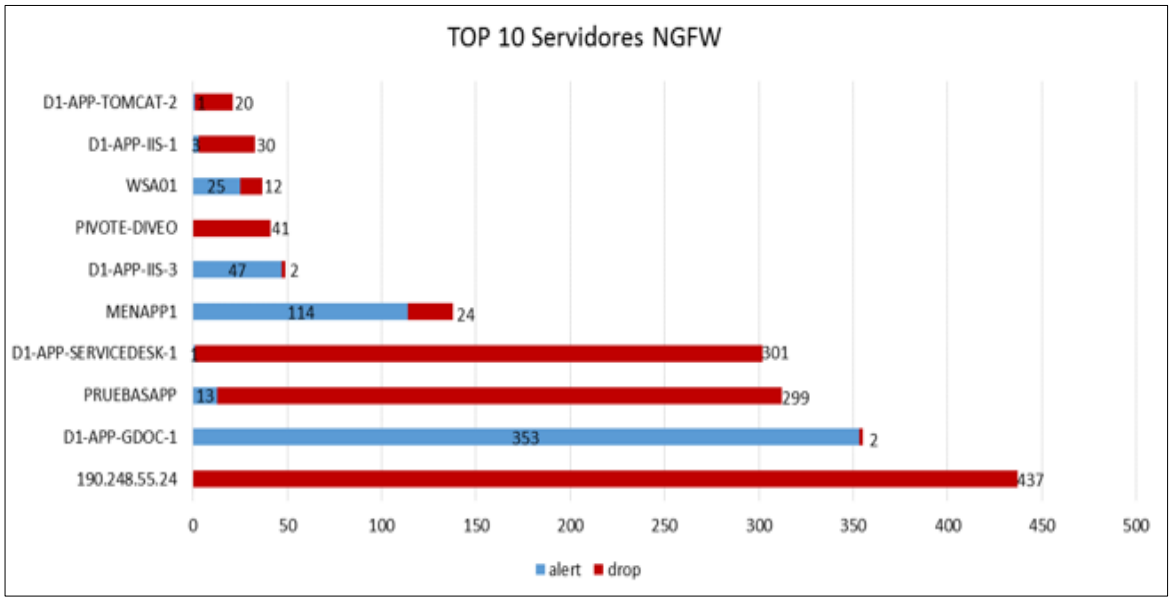


Fuente: Logs NGFW DIVEO mes de septiembre 2016.

Como se observa en la gráfica 73, las 3 firmas con mayor número de eventos son: "*Apache Tomcat Windows Installer Default Account Access Vulnerability (34160), HTTP SQL Injection Attempt (36239) y HTTP SQL Injection Attempt (33338),* con el 52.28%, 19.43% y 5.33% respectivamente del total de eventos detectados, donde las barras azules representan los eventos permitidos y las barras de color rojo los eventos bloqueados catalogados como amenazas.

- **Top de servidores con más eventos**

Gráfica 74. Top servidores con más eventos NGFW DIVEO - septiembre 2016

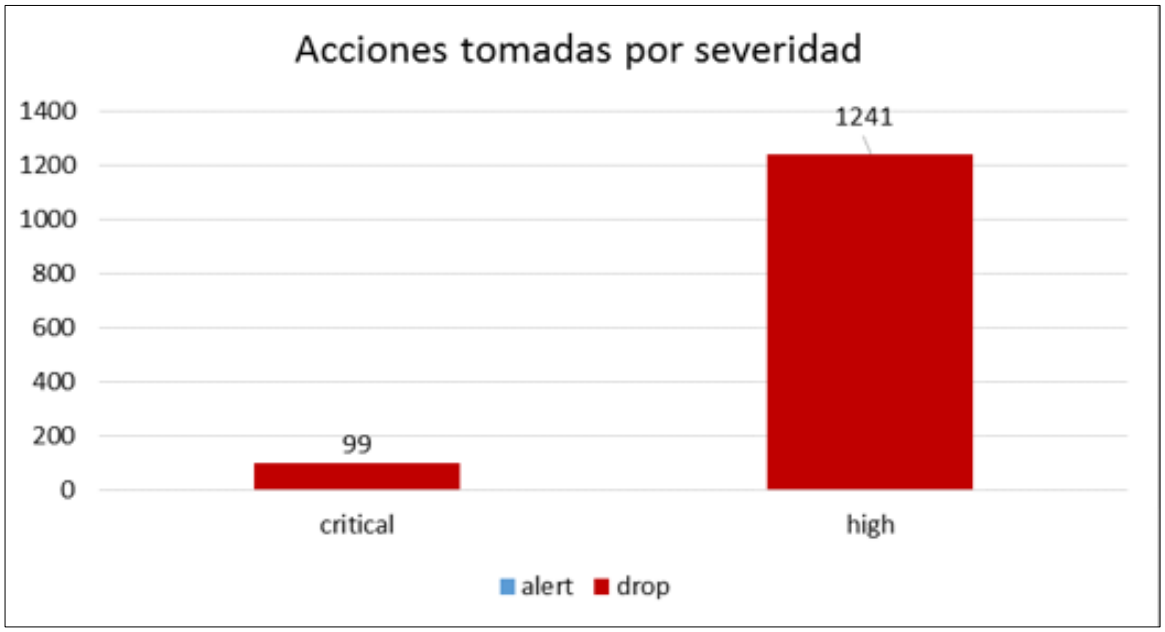


Fuente: Logs NGFW DIVEO mes de septiembre 2016.

Como se observa en la gráfica 74, los 3 servidores con mayor número de eventos son: *"190.248.55.24"* con el 22.4%, *"D1-APP-GDOC-1"* con el 18.2%, y *"PRUEBASAPP"* con el 16% del total de eventos detectados, donde las barras azules representan las firmas permitidas y las barras de color rojo las firmas bloqueadas identificadas como amenazas.

- **Acciones por severidad *critical* y *high***

Gráfica 75. Acciones tomadas por severidad NGFW CAN - septiembre 2016



Fuente: Logs NGFW CAN mes de septiembre 2016.

Como se observa en la gráfica 75, el 100% de las amenazas con severidades *critical* y *high*, están siendo bloqueadas en el NGFW de la sede del CAN.

- **Anti-Virus**

Cuadro 22. Eventos de anti-virus registrado en l el NGFW CAN – septiembre 2016

Firma virus	Eventos
Virus/Win32.Adwind.af (1251891)	9
Virus/Win32.WGeneric.jqrsn (2888881)	9
Trojan/Win32.inject.ihlv (2351780)	6
Virus/Win32.parite.aaxkd (2047976)	5
Virus/Android.WGeneric.jpeyp (1009087)	2
Trojan/AndroidOS.ztorg.gi (1006523)	1
Trojan/Win32.regrun.gulf (2797942)	1
Virus/Win32.virut.gdnda (2458384)	1
Virus/Win32.WGeneric.dulbj (2635006)	1
Total	**35**[56]
Fuente: Logs NGFW CAN mes de septiembre 2016.	

El 100% de las firmas detectadas por el módulo de anti-virus que se observan en el cuadro 22 fueron bloqueadas.

[56] El total refleja la suma de todos los eventos asociados a las firmas de esta categoría y no solamente los mostrados en el TOP 10.

- **Anti-Spyware**

Cuadro 23. Eventos de anti-spyware registrado en el NGFW CAN – septiembre 2016

Firma spyware	Eventos
Xtreme Rat.Gen Command and Control Traffic (13391)	9555
generic:duckdns4.duckdns.org(3816979)	9403
TrojanSpy.nivdort:navstop.ru(3838697)	1078
TrojanSpy.nivdort:againstanabolics.com(3838698)	1058
TrojanSpy.nivdort:cleansportswomen.com(3838437)	1054
TrojanSpy.nivdort:tanzenspielenreiten.org(3835700)	979
generic:nuevochance1.duckdns.org(3819622)	884
generic:hbu5idu6kcgk.mxp2385.com(3808919)	706
Suspicious DNS Query (generic:9786663.com) (4003685)	585
generic:epavypyci.blonderg.com(3812191)	469
Total	**51928**[57]
Fuente: Logs NGFW CAN mes de septiembre 2016.	

Las 3 firmas de anti-spyware con mayor número de eventos, de acuerdo al cuadro 23 son: *"Xtreme Rat.Gen Command and Control Traffic (13391), generic: duckdns4.duckdns.org (3816979) y TrojanSpy.nivdort:navstop.ru (3838697)"*, con el 18.4%, 18.1% y 2.1% respectivamente del total de spyware detectado.

[57] El total refleja la suma de todos los eventos asociados a las firmas de esta categoría y no solamente los mostrados en el TOP 10.

- **Eventos WildFire**

Cuadro 24. Eventos de Wildfire registrado en l el NGFW CAN – septiembre 2016

Servidor	Microsoft MS office (52033)	Microsoft PE file (52060)	Windows executable (EXE) (52020)	Total general
190.248.55.21	33	244	781	1058
50.28.47.31	-	-	168	168
178.79.190.7	-	-	46	46
190.248.55.2	-1	1	25	27
38.111.46.24	-	2	20	22
103.28.12.97	-	1	7	8
203.211.150.27	-	-	7	7
186.24.3.242	-	-	6	6
202.22.203.89	-	2	4	6
202.77.108.170	-	3	3	6
190.248.55.11	-	-	4	4
Total general	**33**	**261**	**1095**	**1390**[58]

Fuente: Logs NGFW CAN mes de septiembre 2016.

Los archivos revisados por el sistema Wildfire, que se observan en el cuadro 24, son objetos con probabilidad de ser maliciosos, que son ejecutados y analizados en un entorno controlado. El sistema Wildfire realiza un diagnóstico, en donde si los archivos recientemente analizados se consideran maliciosos, se genera el reporte y se alimenta el repositorio de Palo Alto.

El 76.1% de los eventos diagnosticados por la nube de Palo Alto como "*malware*" tenían como destino la IP pública 190.248.55.21 recibiendo correos con adjuntos de ejecutables.

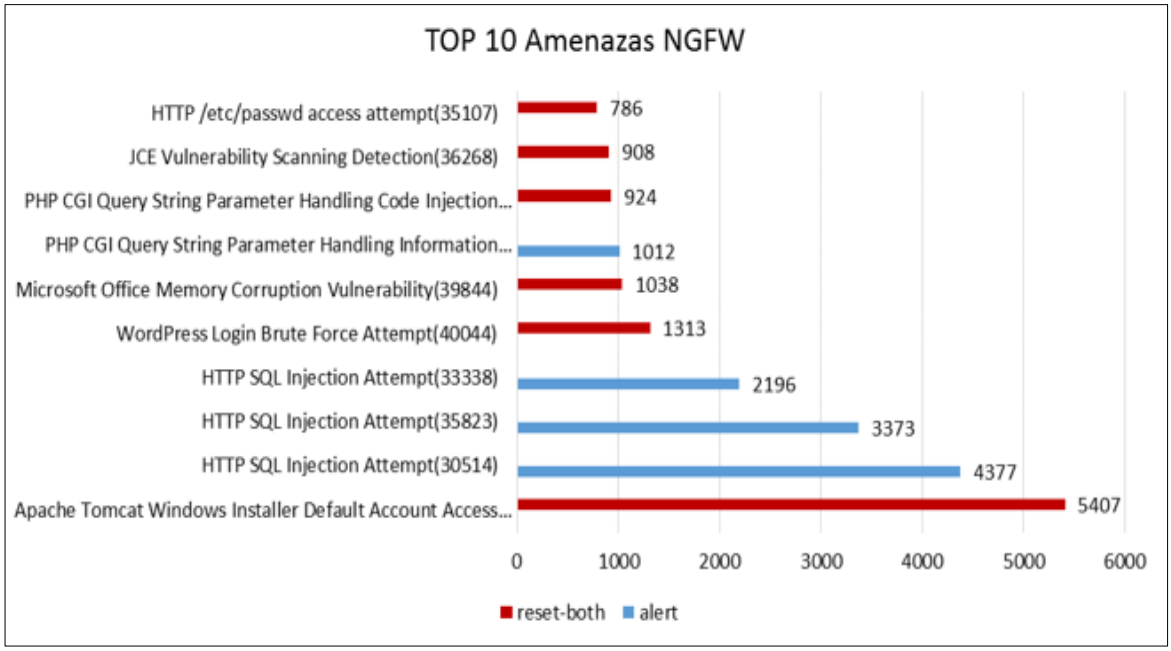
[58] El total refleja la suma de todos los eventos asociados a las firmas de esta categoría y no solamente los mostrados en el TOP 10.

C.6 Reporte mensual estadístico NGFW y WAF – Octubre

DIVEO NGFW

- **Top de amenazas por firma**

Gráfica 76. Top 10 amenazas NGFW DIVEO - octubre 2016

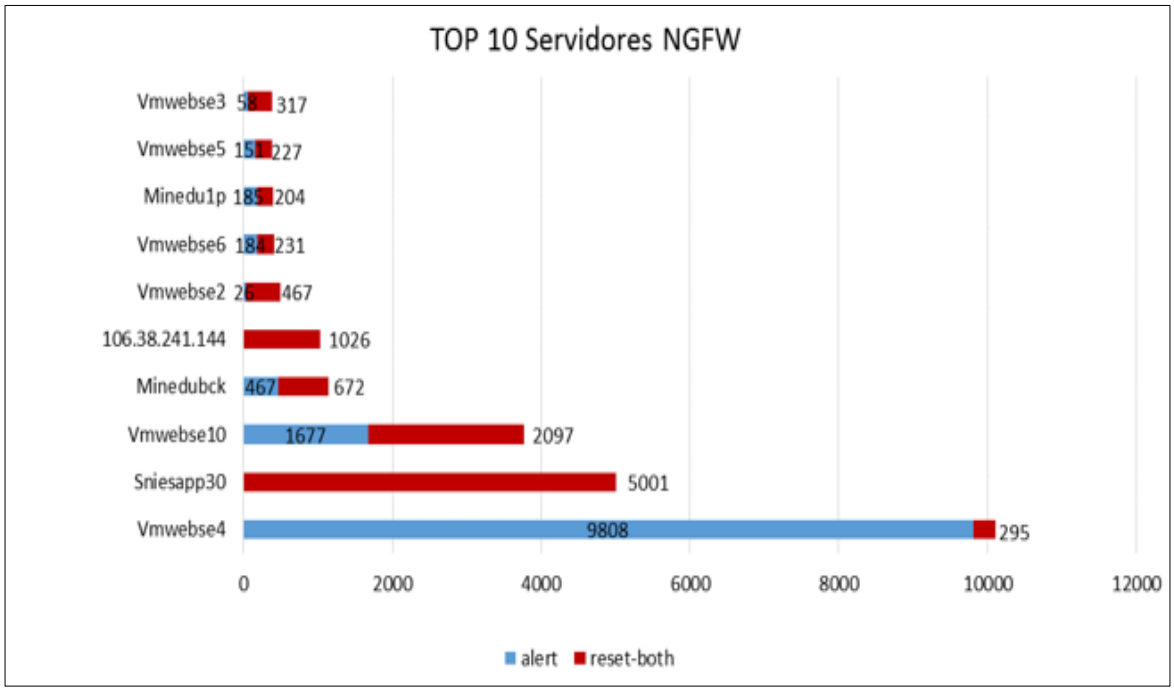


Fuente: Logs NGFW DIVEO mes de octubre 2016.

Como se observa en la gráfica 76, las 3 firmas con mayor número de eventos son: *"Apache Tomcat Windows Installer Default Account Access Vulnerability (34160), HTTP SQL Injection Attempt (30514), y HTTP SQL Injection Attempt (35823)", acumulando* el 21.5%, 17.4% y 13.4% respectivamente del total de eventos detectados, donde las barras azules representan los eventos permitidos y las barras de color rojo los eventos bloqueados catalogados como amenazas.

- **Top de servidores con más eventos**

Gráfica 77. Top servidores con más eventos NGFW DIVEO - octubre 2016

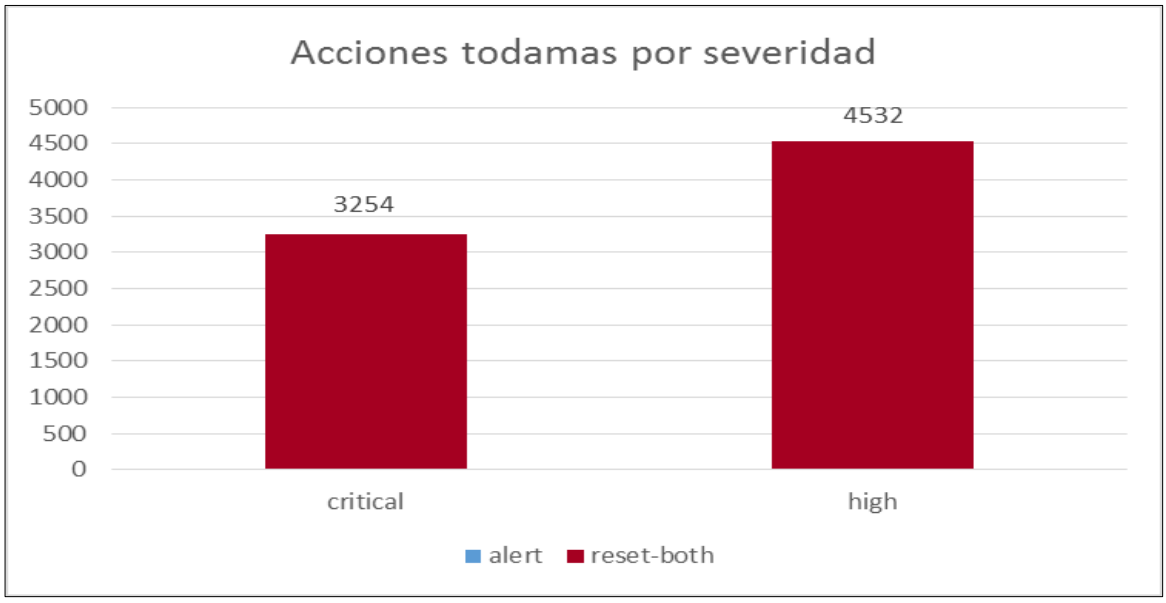


Fuente: Logs NGFW DIVEO mes de octubre 2016.

Como se observa en la gráfica 77, los 3 servidores con mayor número de eventos son: *"Vmwebse4"* con el 40.2%, *"Sniesapp30"* con el 19.9% *y "Vmwebse10"* con el 15% del total de firmas detectadas, donde las barras azules representan las firmas permitidas y las barras de color rojo las firmas bloqueadas identificadas como amenazas.

- **Acciones por severidad *critical* y *high***

Gráfica 78. Acciones tomadas por severidad NGFW DIVEO - octubre 2016



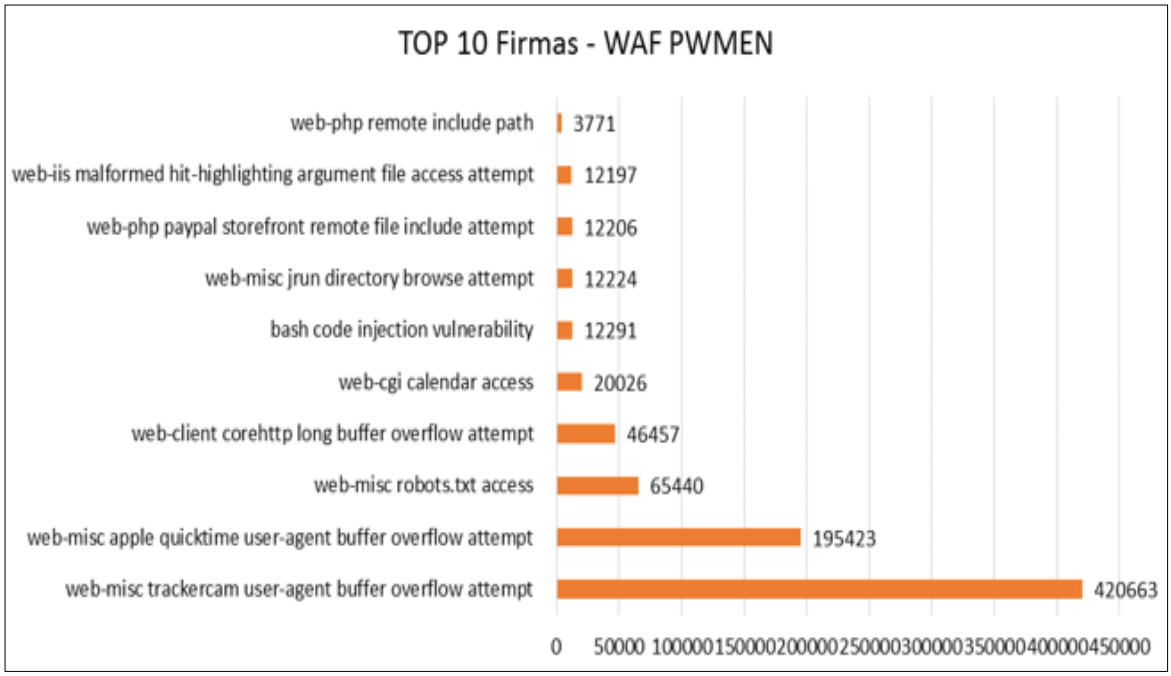
Fuente: Logs NGFW DIVEO mes de octubre 2016.

Como se observa en la gráfica 78, el 100% de las amenazas con severidades *critical* y *high* están siendo bloqueadas en el NGFW de la sede de DIVEO.

DIVEO WAF

- **Top amenazas por firmas**

Gráfica 79. Top 10 firmas WAF - octubre 2016

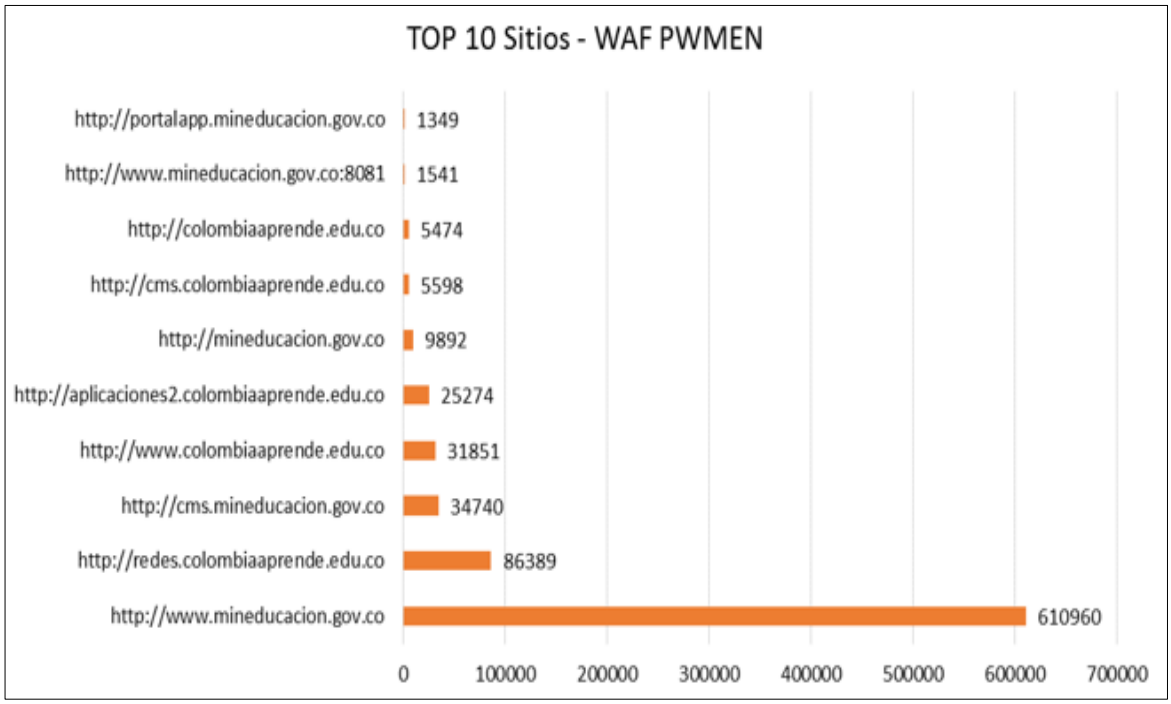


Fuente: Logs WAF mes de octubre 2016.

Como se observa en la gráfica 79, las 3 firmas con mayor número de eventos son: *web-misc trackercam user-agent buffer overflow attempt, web-misc apple quicktime user-agent buffer overflow attempt y web-misc robots.txt access",* con el 51.28%, 23.82% y 7.98% respectivamente del total de eventos presentados.

- **Top sitios web con más eventos**

Gráfica 80. Top 10 sitios WAF - octubre 2016

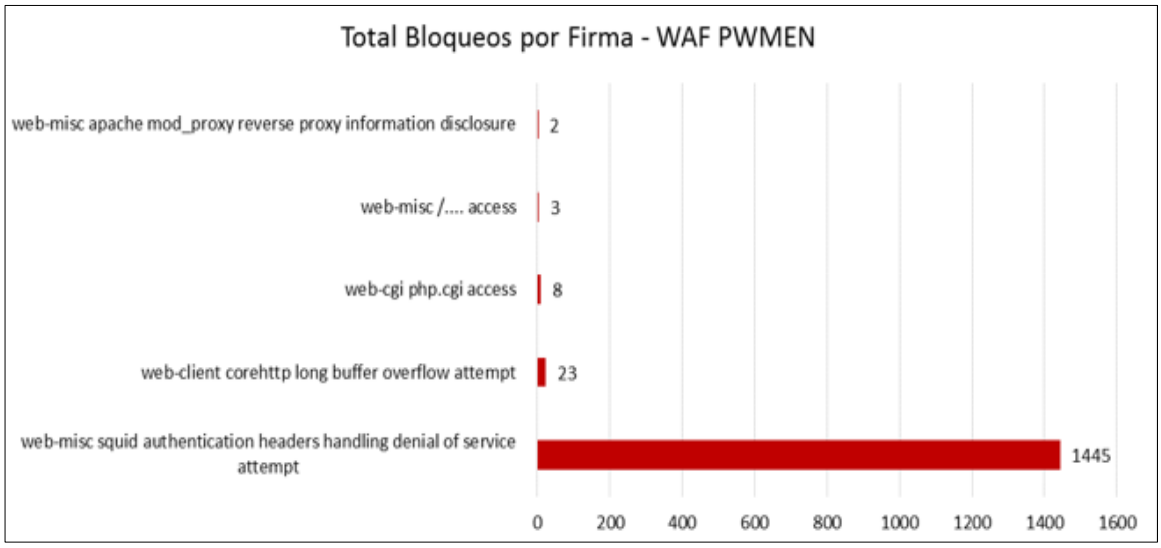


Fuente: Logs WAF mes de octubre 2016.

Los 3 sitios web con mayor número de eventos, de acuerdo a la gráfica 80 son: *"www.mineducacion.gov.co*" con el 74.47%, *"redes.colombiaaprende.edu.co"* con el 10.5%, *y "cms.mineducacion.gov.co"* con el 4.2% del total de eventos presentados.

- **Top bloqueo por firmas**

Gráfica 81. Bloqueo por firmas WAF – octubre 2016

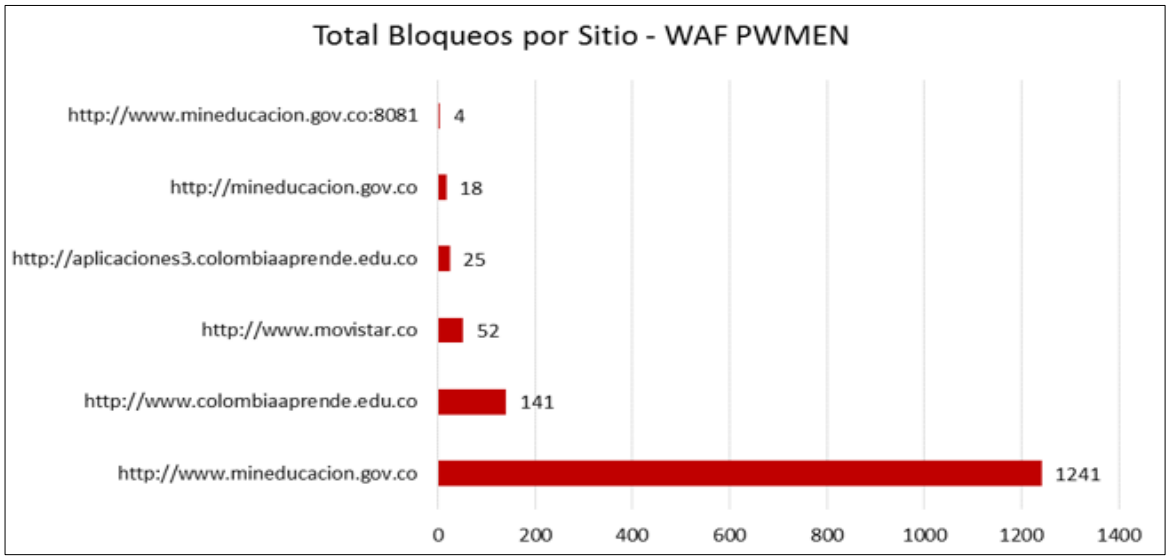


Fuente: Logs WAF mes de octubre 2016.

Como se observa en la gráfica 81, las 3 firmas con mayor número de bloqueos identificadas como amenaza son: "*web-misc squid authentication headers handling denial of service attempt", "web-client corehttp long buffer overflow attempt"* y *"web-cgi php.cgi access*" con el 97.57%, 1.55% y 0.54% respectivamente del total de eventos bloqueados.

- **Top bloqueo por sitios**

Gráfica 82. Bloqueo por sitio WAF – octubre 2016



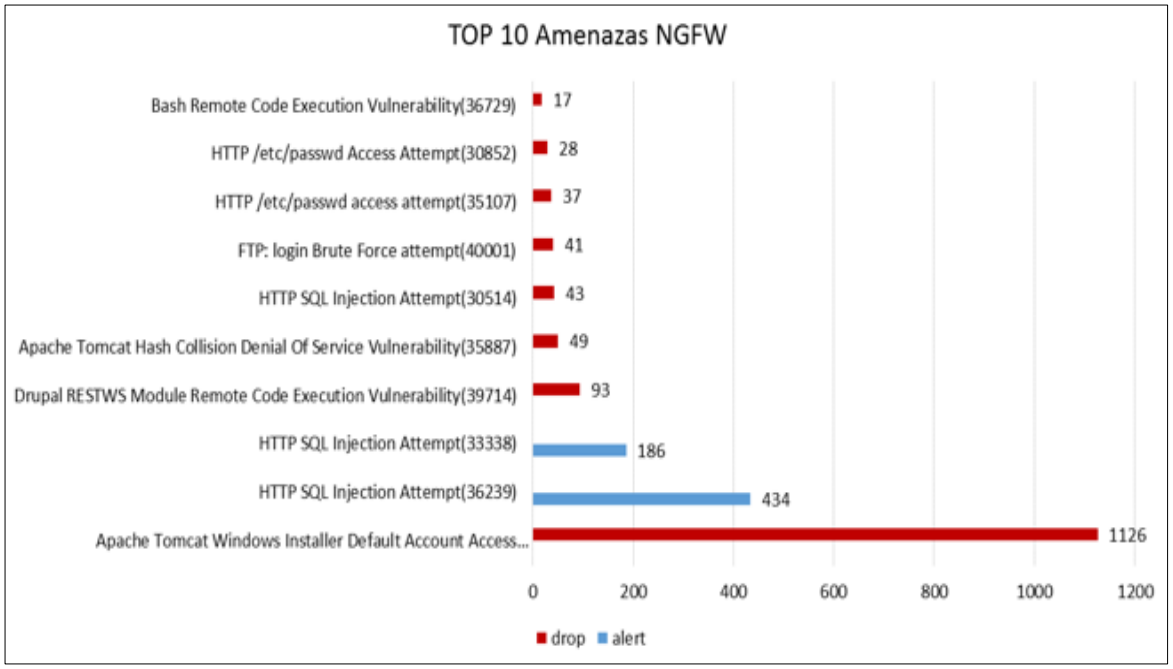
Fuente: Logs WAF mes de octubre 2016.

Como se observa en la gráfica 82, los 3 sitios web con mayor número de firmas bloqueadas identificadas como amenazas son: *"www.mineducacion.gov.co"* con el 83.8%, *"www.colombiaaprende.edu.co"* con el 9.5% y *"www.movistar.co"* con el 3.5% del total de firmas bloqueadas.

CAN NGFW

- **Top de amenazas por firma**

Gráfica 83. Top 10 amenazas NGFW CAN - octubre 2016

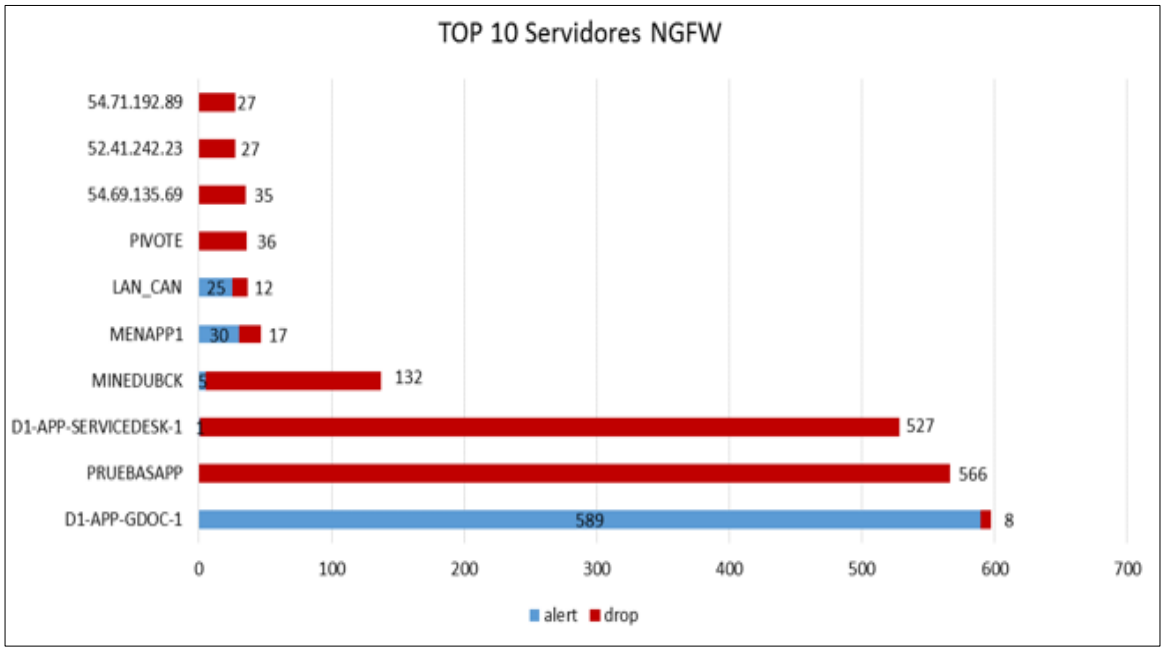


Fuente: Logs NGFW CAN mes de octubre 2016.

Como se observa en la gráfica 83, las 3 firmas con mayor número de eventos son: "*Apache Tomcat Windows Installer Default Account Access Vulnerability (34160)",* "*HTTP SQL Injection Attempt (36239)" y* "*HTTP SQL Injection Attempt (33338)",* acumulando el 51.79%, 19.96% y 8.56% respectivamente del total de eventos detectados, donde las barras azules representan los eventos permitidos y las barras de color rojo los eventos bloqueados catalogados como amenazas.

- **Top de servidores con más eventos**

Gráfica 84. Top servidores con más eventos NGFW CAN - octubre 2016

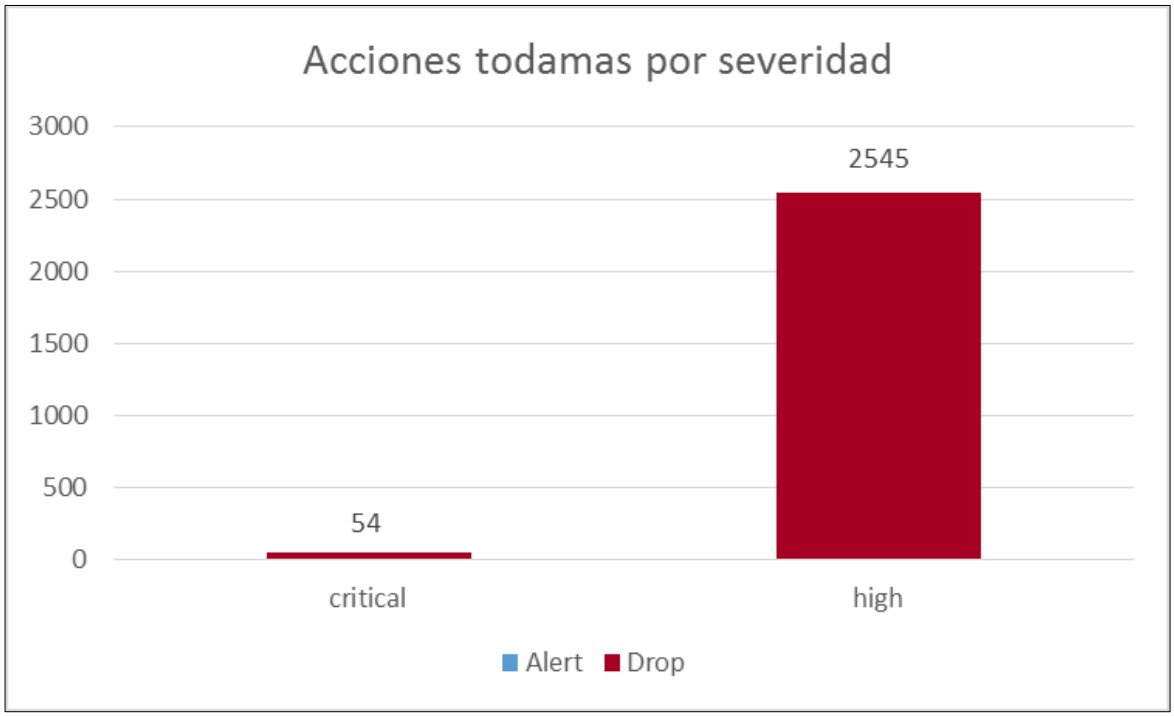


Fuente: Logs NGFW CAN mes de octubre 2016.

Como se observa en la gráfica 84, los 3 servidores con mayor número de eventos son: *"D1-APP-GDOC-1"* con el 27.5%, *"PRUEBASAPP"* con el 26%, y *"D1-APP-SERVICEDESK-1"* con el 24.3% del total de eventos detectados, donde las barras azules representan las firmas permitidas y las barras de color rojo las firmas bloqueadas identificadas como amenazas.

- **Acciones por severidad *critical* y *high***

Gráfica 85. Acciones tomadas por severidad NGFW CAN - octubre 2016



Fuente: Logs NGFW CAN mes de octubre 2016.

Como se observa en la gráfica 85, el 100% de las amenazas con severidades *critical* y *high* están siendo bloqueadas en el NGFW de la sede del CAN.

- **Anti-virus**

Cuadro 25. Eventos de anti-virus registrado en l el NGFW CAN – octubre 2016

Firma virus	Eventos
Virus/Android.malicious.eyod (1007148)	4
Virus/Win32.WGeneric.eeint (1270109)	4
Virus/Win32.malicious.dhmz (1251891)	3
TrojanSpy/Win32.skeeyah.hlu (2627307)	1
Virus/Android.malicious.eyig (1007039)	1
Virus/Win32.malicious.dhlx (1250740)	1
Virus/Win32.WGeneric.kdhnd (2281662)	1
Virus/Win32.WGeneric.kikit (2587559)	1
Virus/Win32.WGeneric.kixzl (2433848)	1
Worm/Win32.allaple.vfinh (2075414)	1
Total	18
Fuente: Logs NGFW CAN mes de octubre 2016.	

El 100% de las firmas detectadas por el módulo de anti-virus que se observan en el cuadro 25 fueron bloqueadas.

- **Anti-Spyware**

Cuadro 26. Eventos de anti-spyware registrado en el NGFW CAN – octubre 2016

Firma spyware	Eventos
Sipvicious.Gen User-Agent Traffic (13272)	110603
Suspicious DNS Query (generic:ginqualzy.hopto.org) (4015907)	25047
generic:duckdns4.duckdns.org(3816979)	12414
Suspicious DNS Query (generic:axpipchxit.ddnsking.com) (4019988)	534
generic:zy371092.gicp.net(3835417)	300
Xtreme Rat.Gen Command and Control Traffic (13391)	234
Morto RDP Request Traffic (13274)	141
Suspicious DNS Query (generic:em.licasd.com) (4044062)	81
Suspicious DNS Query (Trojan.small:www.vissociety.com)(4000101)	72
Win32.Conficker.C p2p (12544)	45
Total	**150821**[59]
Fuente: Logs NGFW CAN mes de octubre 2016.	

Las 3 firmas de anti-spyware con mayor número de eventos, de acuerdo al cuadro 26 son: *"Sipvicious.Gen User-Agent Traffic (13272), Suspicious DNS Query (generic: ginqualzy.hopto.org) (4015907) y generic: duckdns4.duckdns.org (3816979)*", con el 73.3%, 16.6% y 8.2% respectivamente del total de spyware detectado.

[59] El total refleja la suma de todos los eventos asociados a las firmas de esta categoría y no solamente los mostrados en el TOP 10.

- **Eventos WildFire**

Cuadro 27. Eventos de Wildfire registrado en l el NGFW CAN – octubre 2016

Servidor	Microsoft MS office (52033)	Windows executable (EXE) (52020)	Total general
190.248.55.21	-	18	18
50.28.47.31	6	6	12
178.79.190.7	-	4	4
Total general	**5**	**28**	**34**

Fuente: Logs NGFW CAN mes de octubre 2016.

Los archivos revisados por el sistema Wildfire, que se observan en el cuadro 27, son objetos con probabilidad de ser maliciosos, que son ejecutados y analizados en un entorno controlado. El sistema Wildfire realiza un diagnóstico, en donde si los archivos recientemente analizados se consideran maliciosos, se genera el reporte y se alimenta el repositorio de Palo Alto.

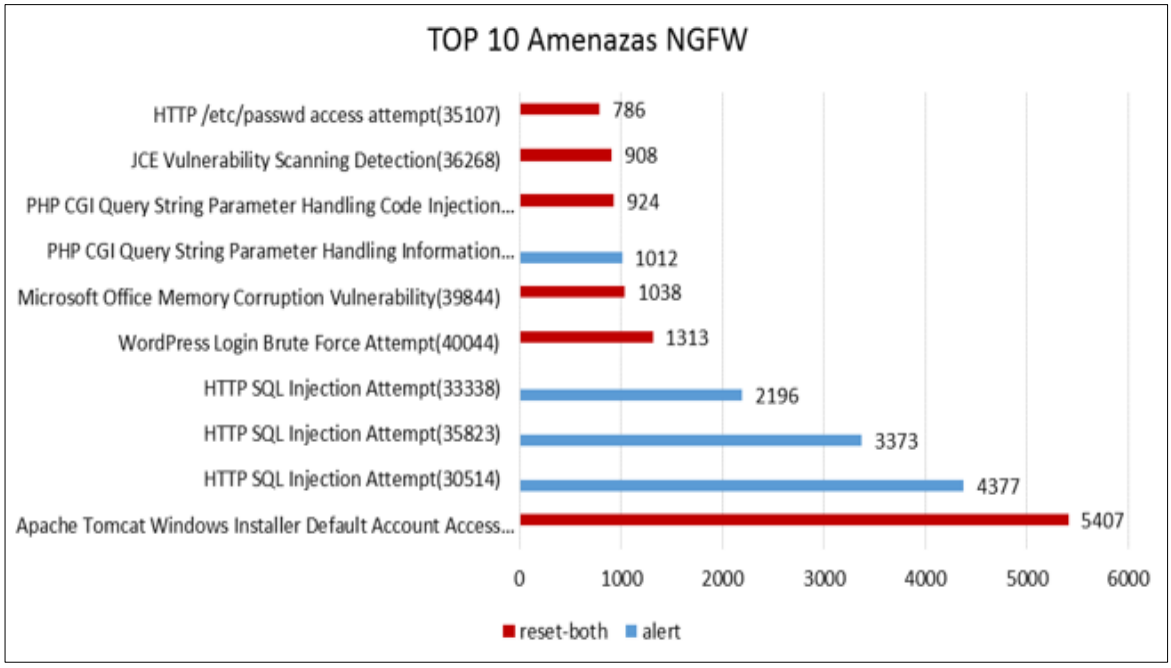
El 35.3% de los eventos diagnosticados por la nube de Palo Alto como "*malware*" tenían como destino la IP pública 190.248.55.21, lo que indica que corresponden a correos electrónicos con archivos ejecutables de carácter malicioso.

C.7 Reporte mensual estadístico NGFW y WAF – Noviembre

DIVEO NGFW

- **Top de amenazas por firma**

Gráfica 86. Top 10 amenazas NGFW DIVEO - noviembre 2016

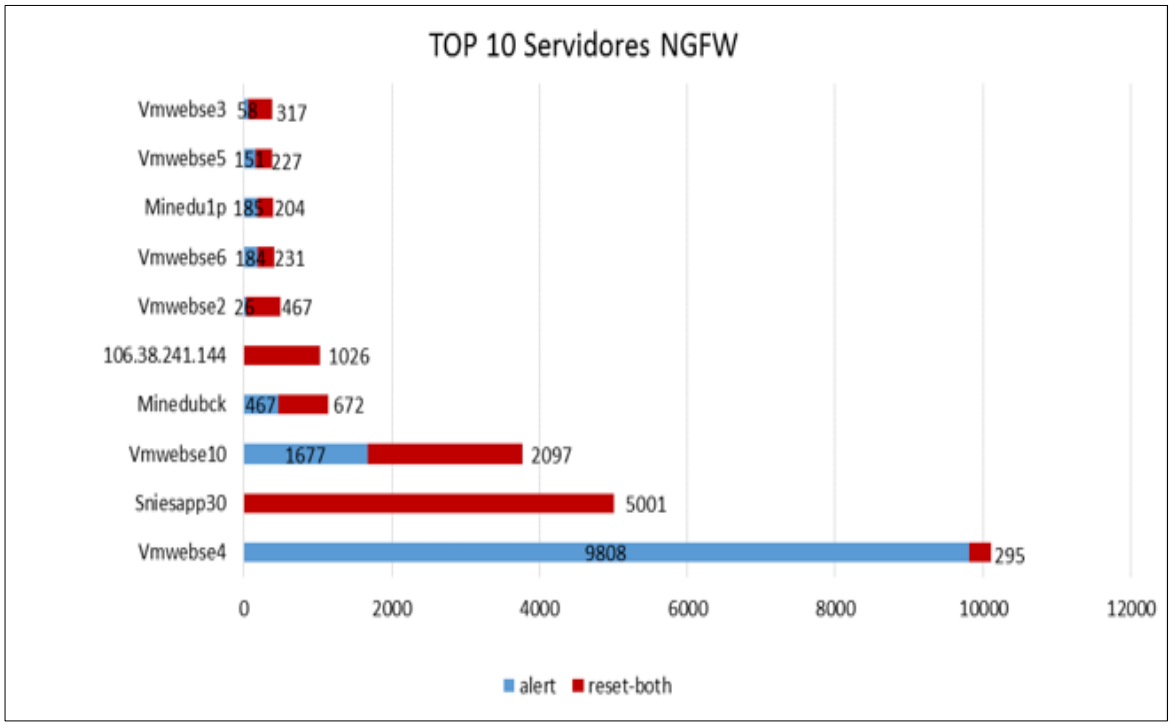


Fuente: Logs NGFW DIVEO mes de noviembre 2016.

Como se observa en la gráfica 86, las 3 firmas con mayor número de eventos son: *"Apache Tomcat Windows Installer Default Account Access Vulnerability (34160), HTTP SQL Injection Attempt (30514), y HTTP SQL Injection Attempt (35823)", acumulando* el 21.5%, 17.4% y 13.4% respectivamente del total de eventos detectados, donde las barras azules representan los eventos permitidos y las barras de color rojo los eventos bloqueados catalogados como amenazas.

- **Top de servidores con más eventos**

Gráfica 87. Top servidores con más eventos NGFW DIVEO - noviembre 2016

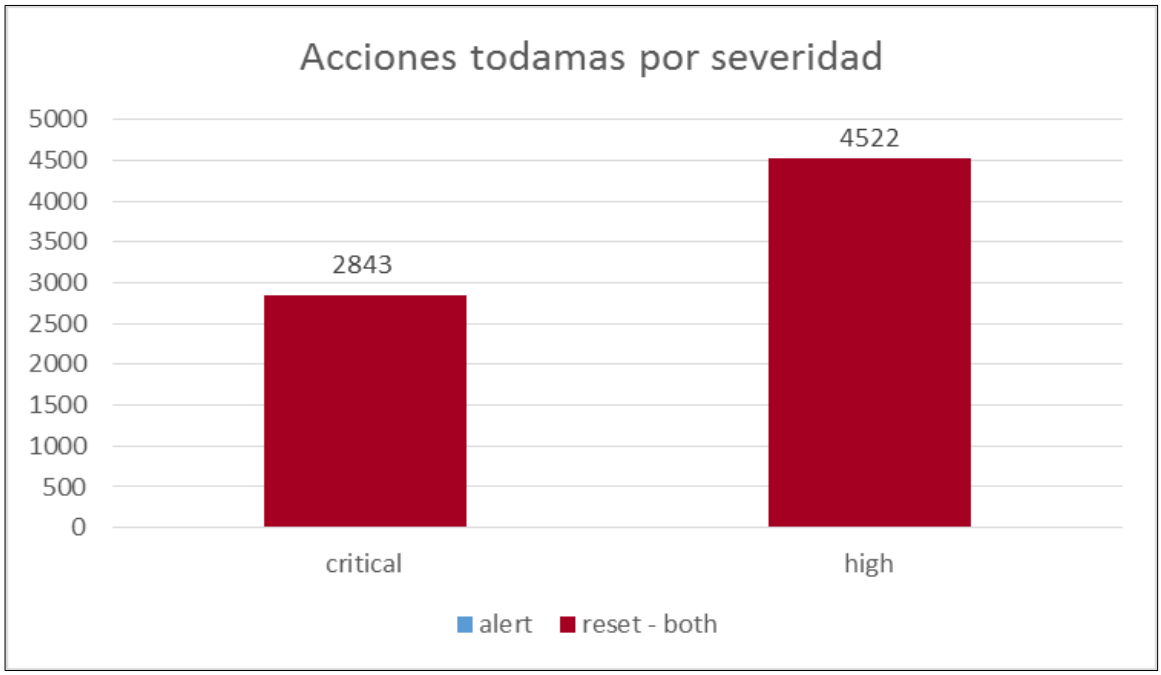


Fuente: Logs NGFW DIVEO mes de noviembre 2016.

Como se observa en la gráfica 87, los 3 servidores con mayor número de eventos son: *"Vmwebse4"* con el 40.2%, *"Sniesapp30"* con el 19.9% *y "Vmwebse10"* con el 15.1% del total de eventos detectados, donde las barras azules representan las firmas permitidas y las barras de color rojo las firmas bloqueadas identificadas como amenazas.

- **Acciones por severidad *critical* y *high***

Gráfica 88. Acciones tomadas por severidad NGFW DIVEO - noviembre 2016



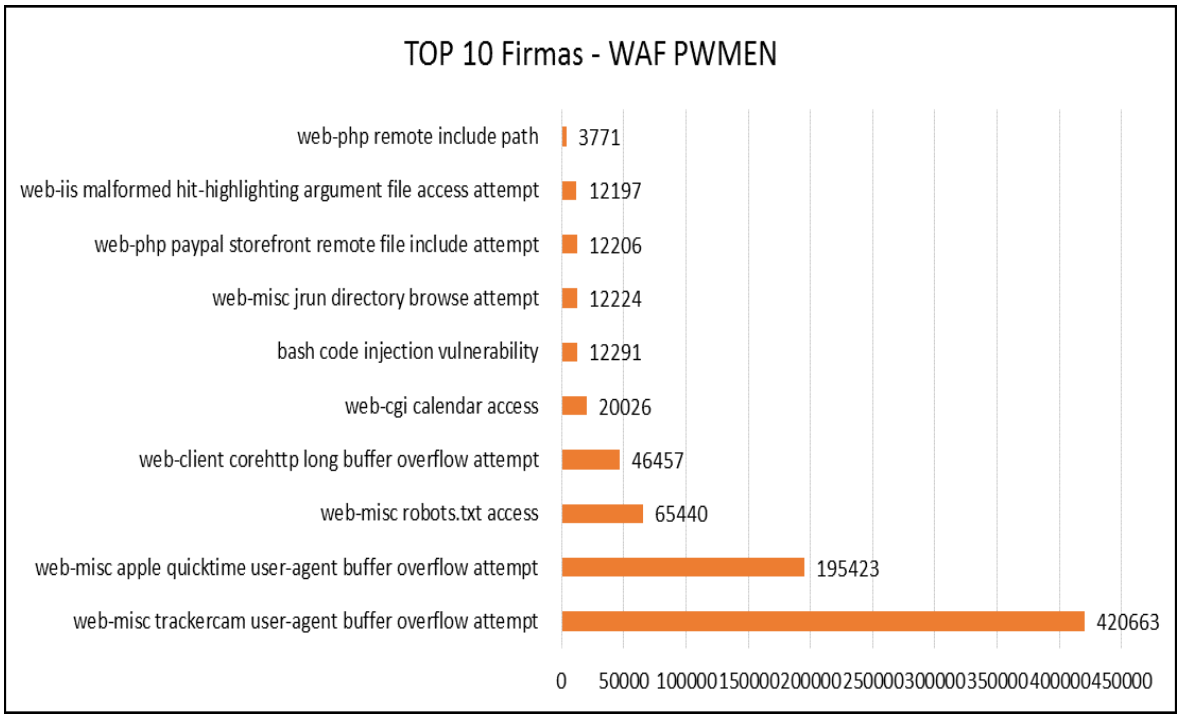
Fuente: Logs NGFW DIVEO mes de noviembre 2016.

Como se observa en la gráfica 88, el 100% de las amenazas con severidades *critical* y *high* están siendo bloqueadas en el NGFW de la sede de DIVEO.

DIVEO WAF

- **Top amenazas por firmas**

Gráfica 89. Top 10 firmas WAF - noviembre 2016

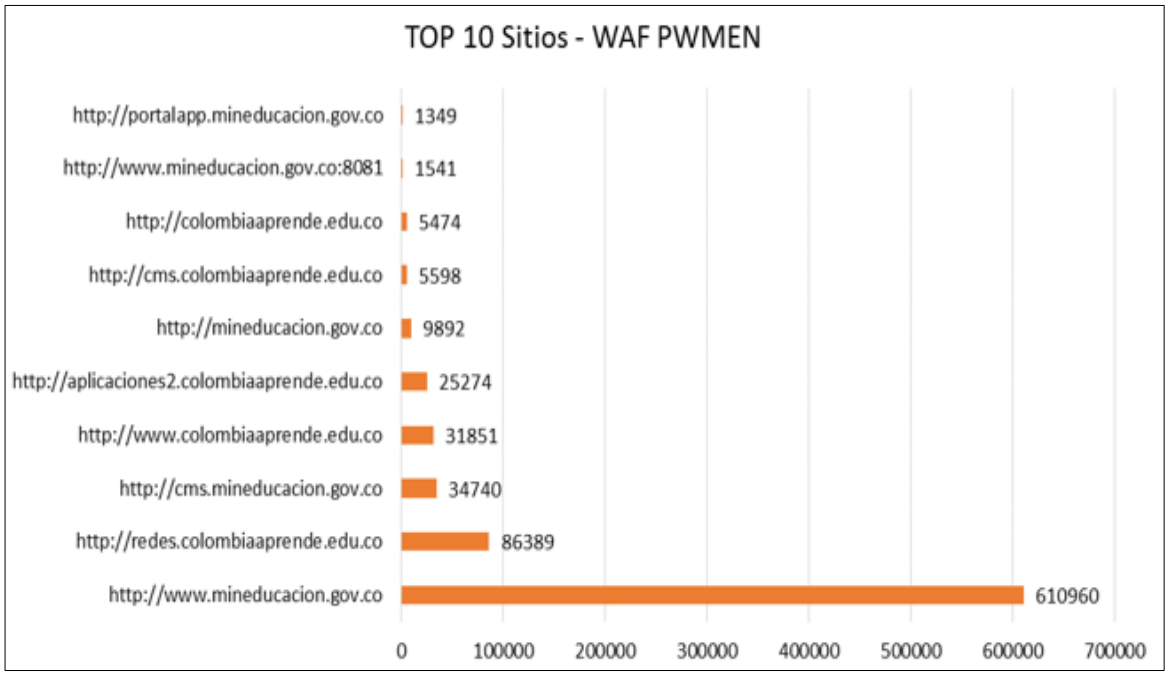


Fuente: Logs WAF mes de noviembre 2016.

Como se observa en la gráfica 89, las 3 firmas con mayor número de eventos son: *web-misc trackercam user-agent buffer overflow attempt, web-misc apple quicktime user-agent buffer overflow attempt y web-misc robots.txt access",* con el 51.28%, 23.82% y 7.98% respectivamente del total de eventos presentados.

- **Top sitios web con más eventos**

Gráfica 90. Top 10 sitios WAF - noviembre 2016

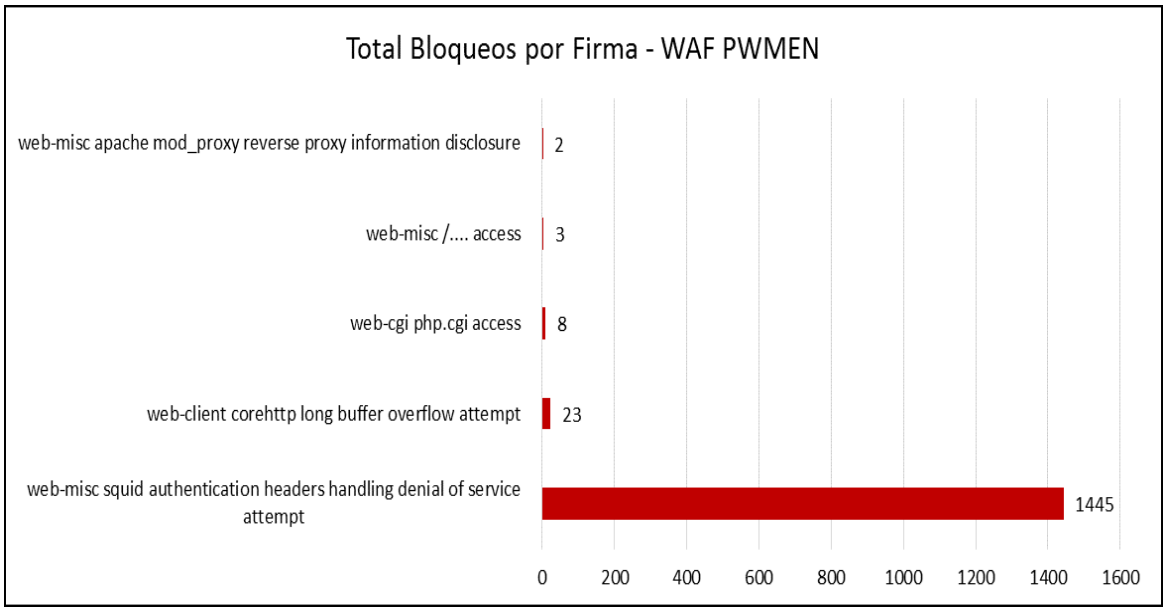


Fuente: Logs WAF mes de noviembre 2016.

Los 3 sitios web con mayor número de eventos, de acuerdo a la gráfica 90 son: "*www.mineducacion.gov.co"* con el 74.5%*, "redes.colombiaaprende.edu.co"* con el 10.5%*, y "cms.mineducacion.gov.co"* con el 4.2% del total de eventos presentados.

- **Top bloqueo por firma**

Gráfica 91. Bloqueo por firmas WAF – noviembre 2016

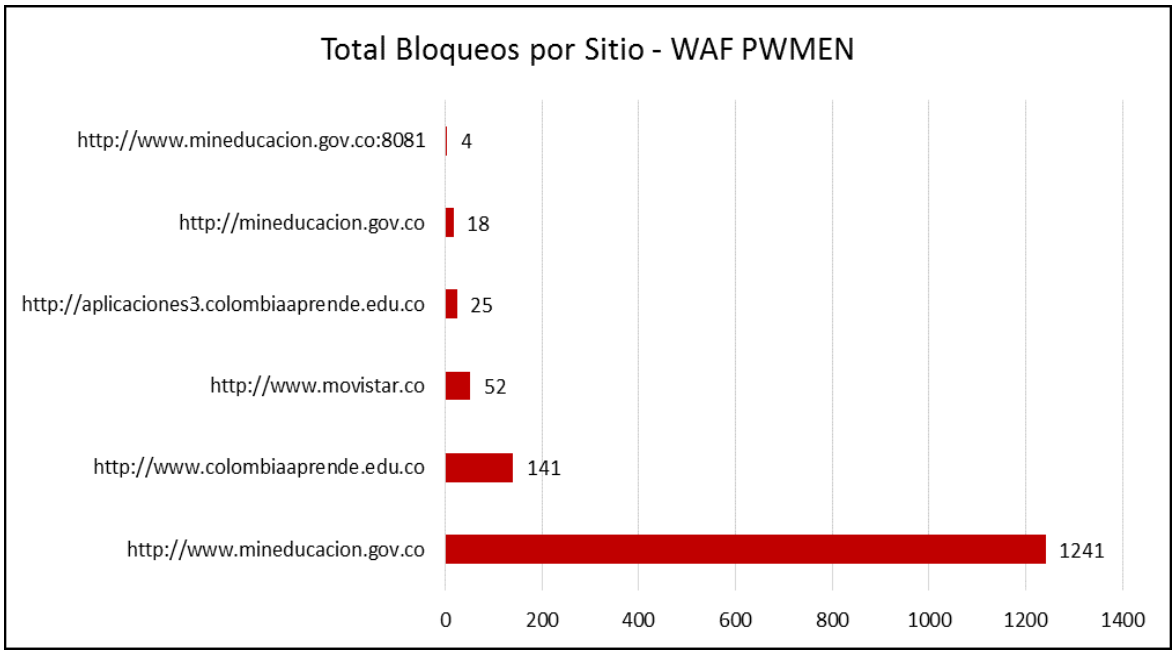


Fuente: Logs WAF mes de noviembre 2016.

Como se observa en la gráfica 91, las 3 firmas con mayor número de bloqueos son: *"web-misc squid authentication headers handling denial of service attempt, web-client corehttp long buffer overflow attempt y web-cgi php.cgi access"* con el 97.57%, 1.55% y 0.54% respectivamente del total de eventos bloqueados.

- **Top bloqueo por sitios**

Gráfica 92. Bloqueo por sitio WAF – noviembre 2016



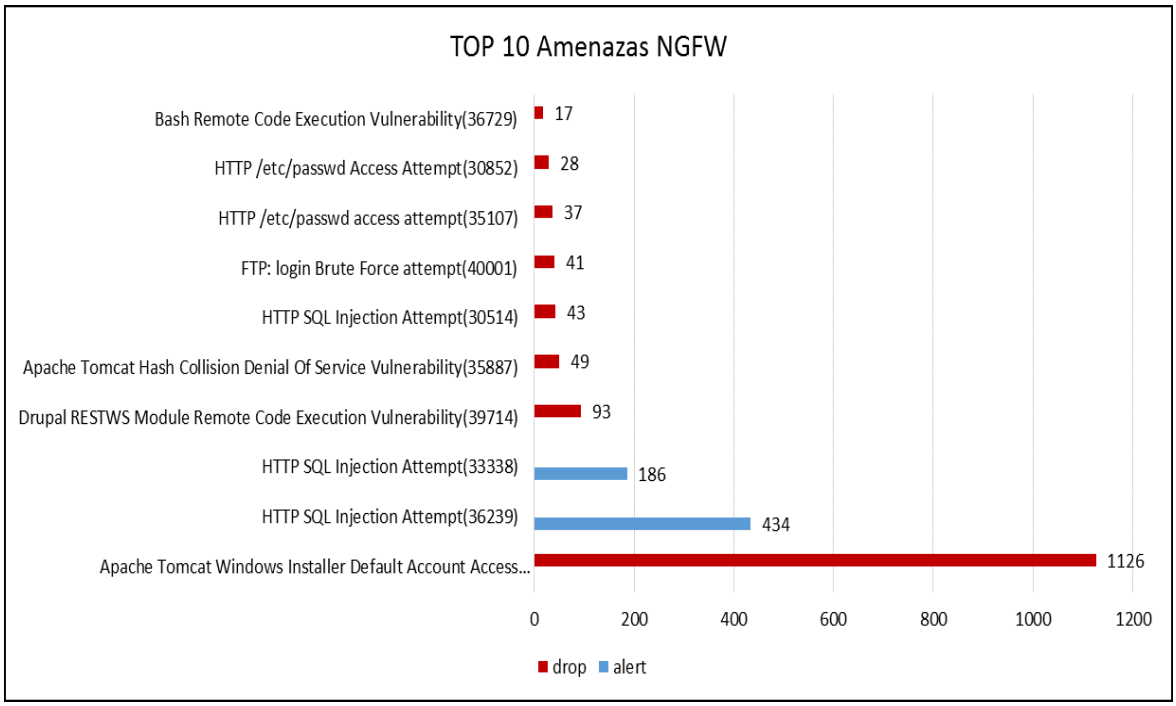
Fuente: Logs WAF mes de noviembre 2016.

Como se observa en la gráfica 92, los 3 sitios web con mayor número de firmas bloqueadas identificadas como amenazas son: *"www.mineducacion.gov.co"* con el 83.79%, *"www.colombiaaprende.edu.co"* con el 9.52% y *"www.movistar.co"* con el 3.51% del total de firmas bloqueadas.

CAN NGFW

- **Top de amenazas por firma**

Gráfica 93. Top 10 amenazas NGFW CAN - noviembre 2016

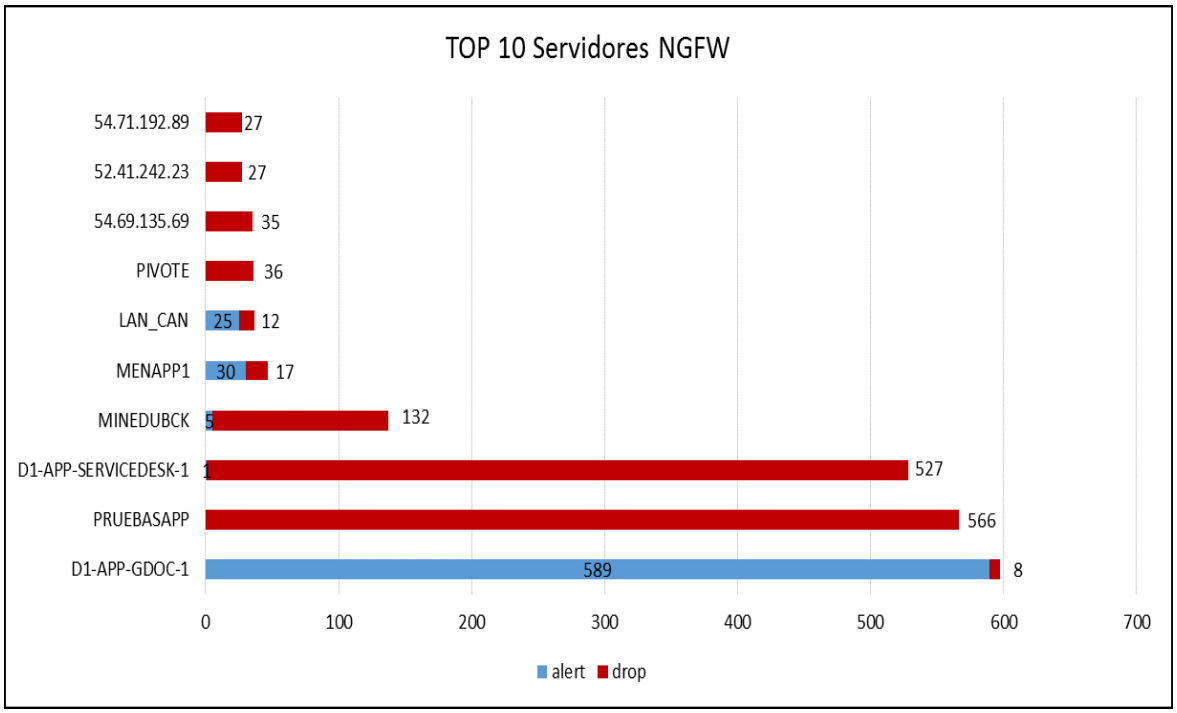


Fuente: Logs NGFW DIVEO mes de noviembre 2016.

Como se observa en la gráfica 93, las 3 firmas con mayor número de eventos son: "*Apache Tomcat Windows Installer Default Account Access Vulnerability (34160), HTTP SQL Injection Attempt (36239) y HTTP SQL Injection Attempt (33338),* con el 51.79%, 19.96% y 8.56% respectivamente del total de eventos detectados, donde la barra azul representan los eventos permitidos y la barra de color rojo los eventos bloqueados catalogados como amenazas.

- **Top de servidores con más eventos**

Gráfica 94. Top servidores con más eventos NGFW CAN - noviembre 2016

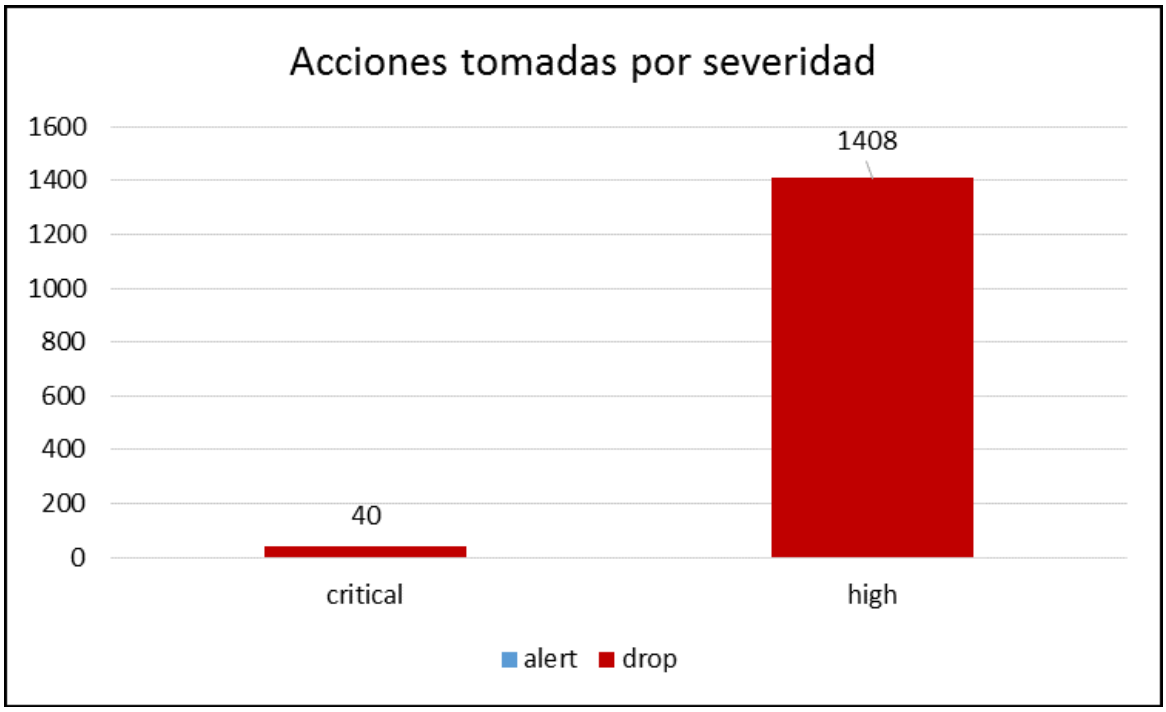


Fuente: Logs NGFW CAN mes de noviembre 2016.

Como se observa en la gráfica 94, los 3 servidores con mayor número de eventos son: *"D1-APP-GDOC-1"* con el 27.4%, *"PRUEBASAPP"* con el 26%, y *"D1-APP-SERVICEDESK-1"* con el 24.3% del total de eventos detectados, donde las barras azules representan las firmas permitidas y las barras de color rojo las firmas bloqueadas identificadas como amenazas.

- **Acciones por severidad *critical* y *high***

Gráfica 95. Acciones tomadas por severidad NGFW CAN - noviembre 2016



Fuente: Logs NGFW CAN mes de noviembre 2016.

Como se observa en la gráfica 95, el 100% de las amenazas con severidades *critical* y *high* están siendo bloqueadas en el NGFW de la sede del CAN.

- **Anti-Virus**

Cuadro 28. Eventos de anti-virus registrado en l el NGFW CAN – noviembre 2016

Firma virus	Eventos
Virus/Android.malicious.eyod (1007148)	4
Virus/Win32.WGeneric.eeint (1270109)	4
Virus/Win32.malicious.dhmz (1251891)	3
TrojanSpy/Win32.skeeyah.hlu (2627307)	1
Virus/Android.malicious.eyig (1007039)	1
Virus/Win32.malicious.dhlx (1250740)	1
Worm/Win32.allaple.vfinh (2075414)	1
Total	**15**
Fuente: Logs NGFW CAN mes de noviembre 2016.	

El 100% de las firmas detectadas por el módulo de anti-virus que se observan en el cuadro 28 fueron bloqueadas.

- **Anti-Spyware**

Cuadro 29. Eventos de anti-spyware registrado en el NGFW CAN – noviembre 2016

Firma spyware	Eventos
Sipvicious.Gen User-Agent Traffic (13272)	110603
Suspicious DNS Query (generic:ginqualzy.hopto.org) (4015907)	25047
generic:duckdns4.duckdns.org(3816979)	12414
Suspicious DNS Query (generic:axpipchxit.ddnsking.com) (4019988)	534
generic:zy371092.gicp.net(3835417)	304
Xtreme Rat.Gen Command and Control Traffic (13391)	234
Suspicious DNS Query (generic:em.licasd.com) (4044062)	81
Win32.Conficker.C p2p (12544)	47
Total	**120351**[60]
Fuente: Logs NGFW CAN mes de noviembre 2016.	

Las 3 firmas de anti-spyware con mayor número de eventos, de acuerdo al cuadro 29 son: *"Sipvicious.Gen User-Agent Traffic (13272), Suspicious DNS Query (generic: ginqualzy.hopto.org) (4015907) y generic: duckdns4.duckdns.org (3816979)"*, con el 73.33%, 16.61% y 8.23% respectivamente del total de spyware detectado.

[60] El total refleja la suma de todos los eventos asociados a las firmas de esta categoría y no solamente los mostrados en el TOP 10.

- **Eventos WildFire**

Cuadro 30. Eventos de Wildfire registrado en l el NGFW CAN – noviembre 2016

Servidor	Microsoft MS office (52033)	Windows executable (EXE) (52020)	Total general
190.248.55.21	-	18	18
50.28.47.31	6	6	12
178.79.190.7	-	4	4
Total general	**5**	**28**	**34**

Fuente: Logs NGFW CAN mes de noviembre 2016.

Los archivos revisados por el sistema Wildfire, que se observan en el cuadro 30, son objetos con probabilidad de ser maliciosos, que son ejecutados y analizados en un entorno controlado. El sistema Wildfire realiza un diagnóstico, en donde si los archivos recientemente analizados se consideran maliciosos, se genera el reporte y se alimenta el repositorio de Palo Alto.

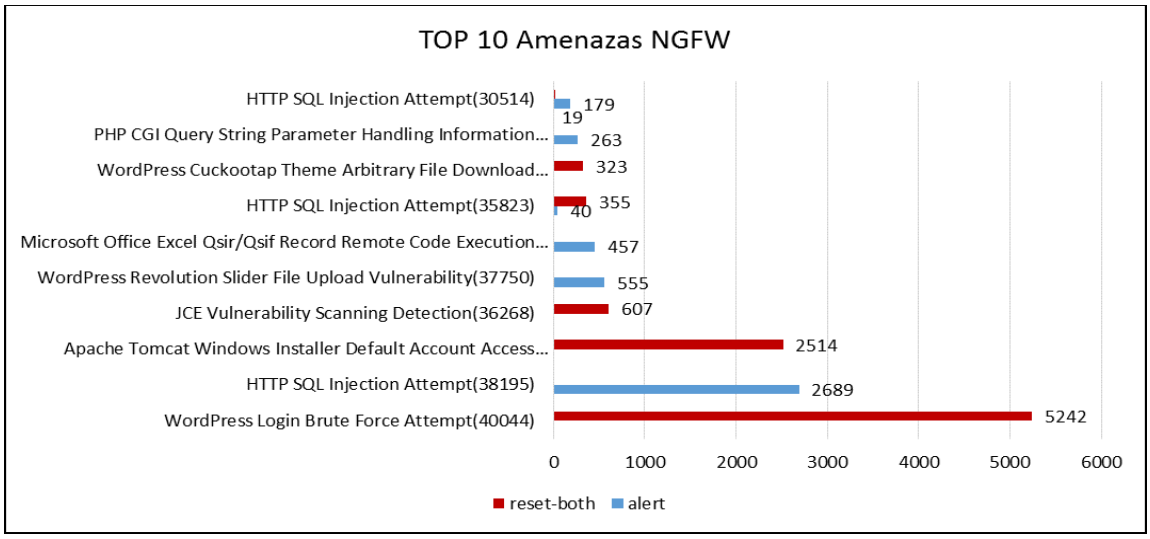
El 35.3% de los eventos diagnosticados por la nube de Palo Alto como "*malware*" tenían como destino la IP pública 190.248.55.21, lo que indica que corresponden a correos electrónicos con archivos ejecutables de carácter malicioso.

C.8 Reporte mensual estadístico NGFW y WAF – Diciembre

DIVEO NGFW

- **Top de amenazas por firma**

Gráfica 96. Top 10 amenazas NGFW DIVEO - diciembre 2016

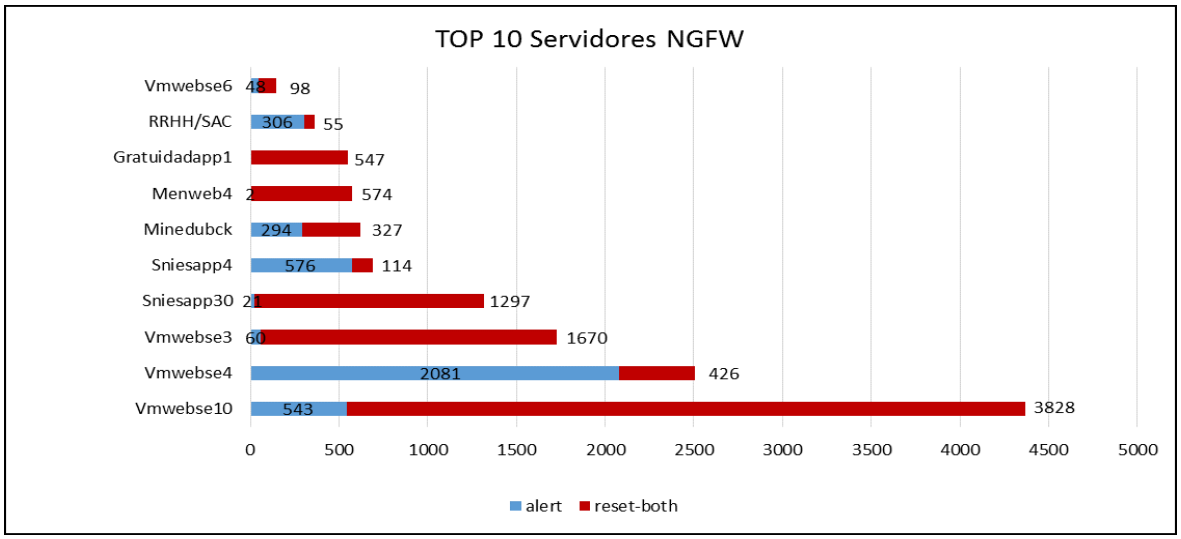


Fuente: Logs NGFW DIVEO mes de diciembre 2016.

Como se observa en la gráfica 96, las 3 firmas con mayor número de eventos son: *"WordPress Login Brute Force Attempt (40044), HTTP SQL Injection Attempt (38195), y Apache Tomcat Windows Installer Default Account Access Vulnerability (34160)",* con el 35.98%, 18.46% y 17.26% respectivamente del total de eventos detectados, donde las barras azules representan los eventos permitidos y las barras de color rojo los eventos bloqueados catalogados como amenazas.

- **Top de servidores con más eventos**

Gráfica 97. Top servidores con más eventos NGFW DIVEO - diciembre 2016

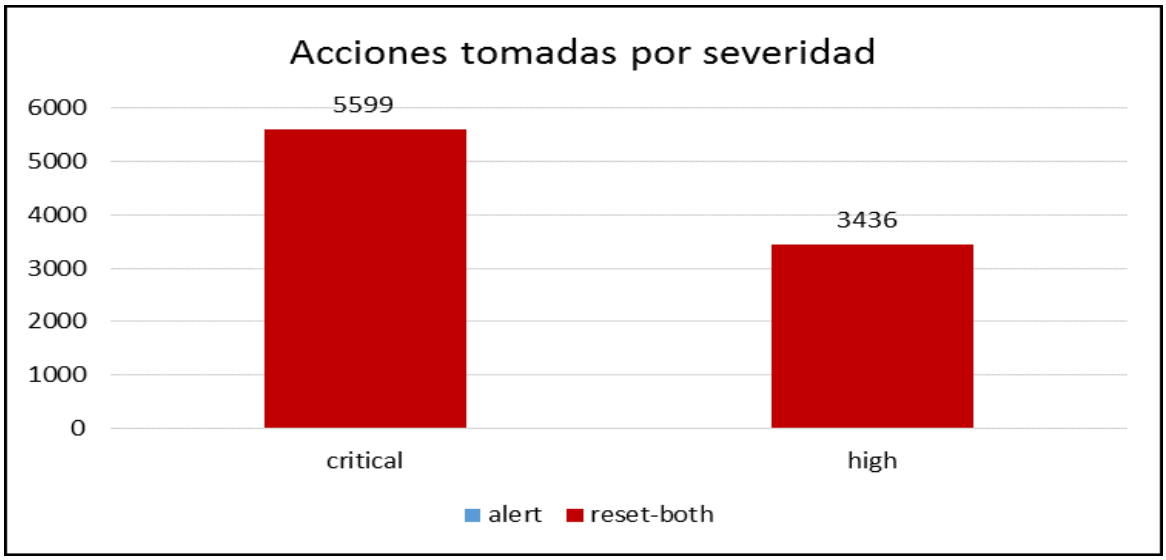


Fuente: Logs NGFW DIVEO mes de diciembre 2016.

Como se observa en la gráfica 97, los 3 servidores con mayor número de eventos son: *"Vmwebse10"* con el 30%, *"Vmwebse4"* con el 17.2% *y "Vmwebse3"* con el 11.9% del total de amenazas detectadas, donde las barras azules representan las firmas permitidas y las barras de color rojo las firmas bloqueadas identificadas como amenazas.

- **Acciones por severidad *critical* y *high***

Gráfica 98. Acciones tomadas por severidad NGFW DIVEO - diciembre 2016



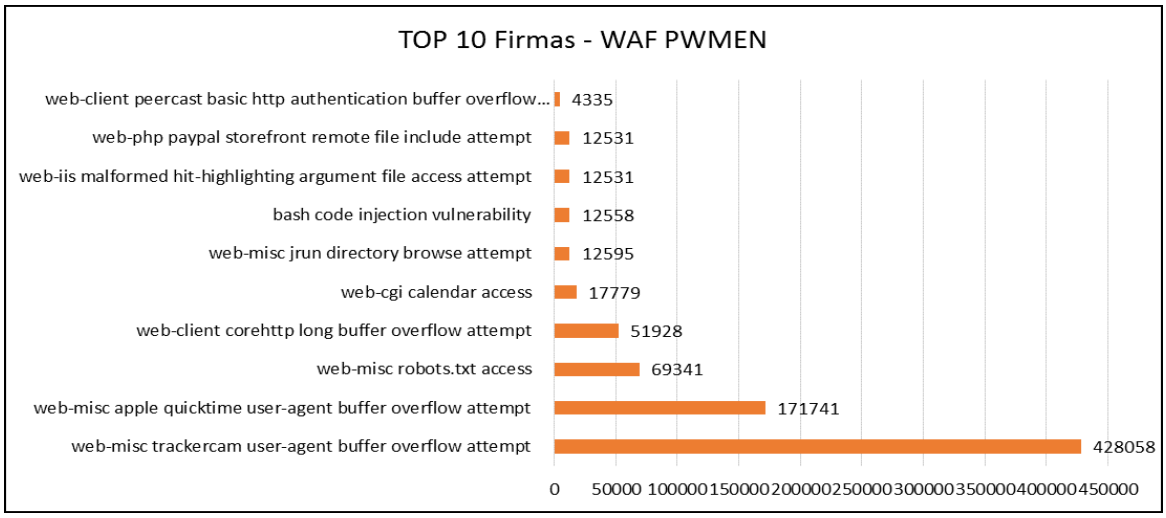
Fuente: Logs NGFW DIVEO mes de diciembre 2016.

Como se observa en la gráfica 98, el 100% de las amenazas con severidades *critical* y *high* están siendo bloqueadas en el NGFW de la sede de DIVEO.

DIVEO WAF

- **Top amenazas por firmas**

Gráfica 99. Top 10 firmas WAF - diciembre 2016

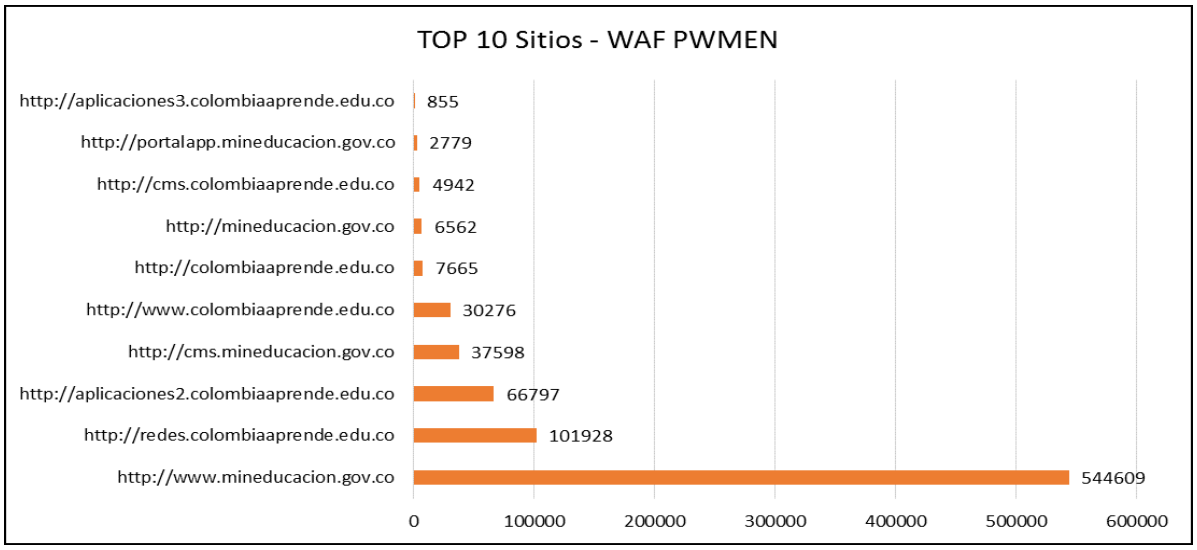


Fuente: Logs WAF mes de diciembre 2016.

Como se observa en la gráfica 99, las 3 firmas con mayor número de eventos son: *web-misc trackercam user-agent buffer overflow attempt, web-misc apple quicktime user-agent buffer overflow attempt y web-misc robots.txt access",* con el 52.91%, 21.23% y 8.57% respectivamente del total de eventos presentados.

- **Top sitios web con más eventos**

Gráfica 100. Top 10 sitios WAF - diciembre 2016

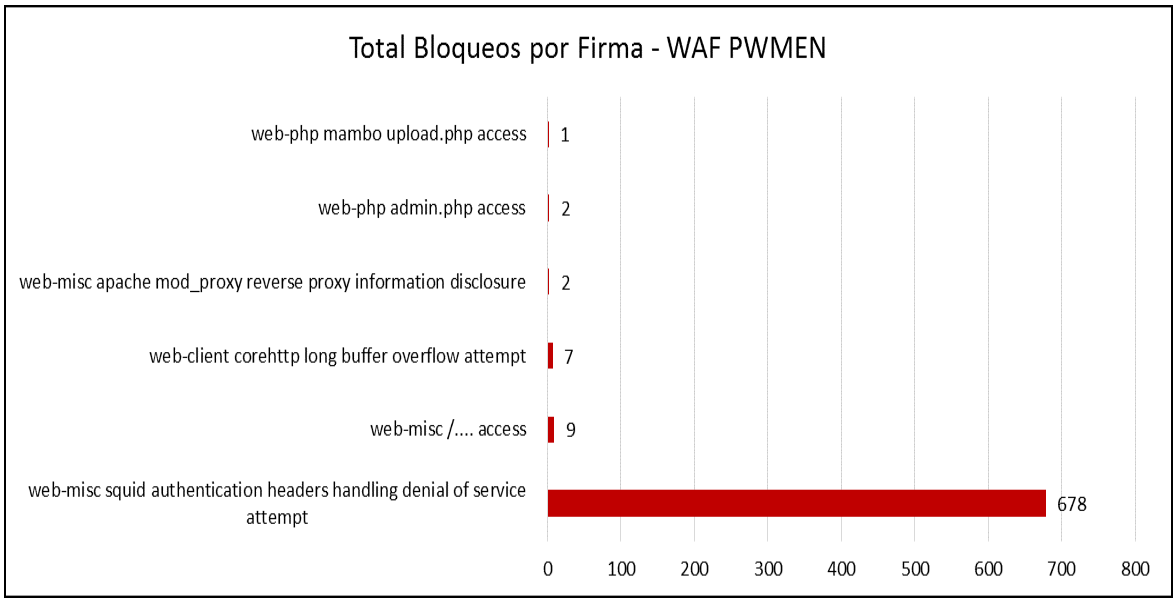


Fuente: Logs WAF mes de diciembre 2016.

Los 3 sitios web con mayor número de eventos, de acuerdo a la gráfica 100 son: "*www.mineducacion.gov.co"* con el 67.32%, *"redes.colombiaaprende.edu.co"* con el 12.6%, *y "aplicaciones2.colombiaaprende.edu.co"* con el 8.26% del total de eventos presentados.

- **Top bloqueo por firmas**

Gráfica 101. Bloqueo por firmas WAF – diciembre 2016

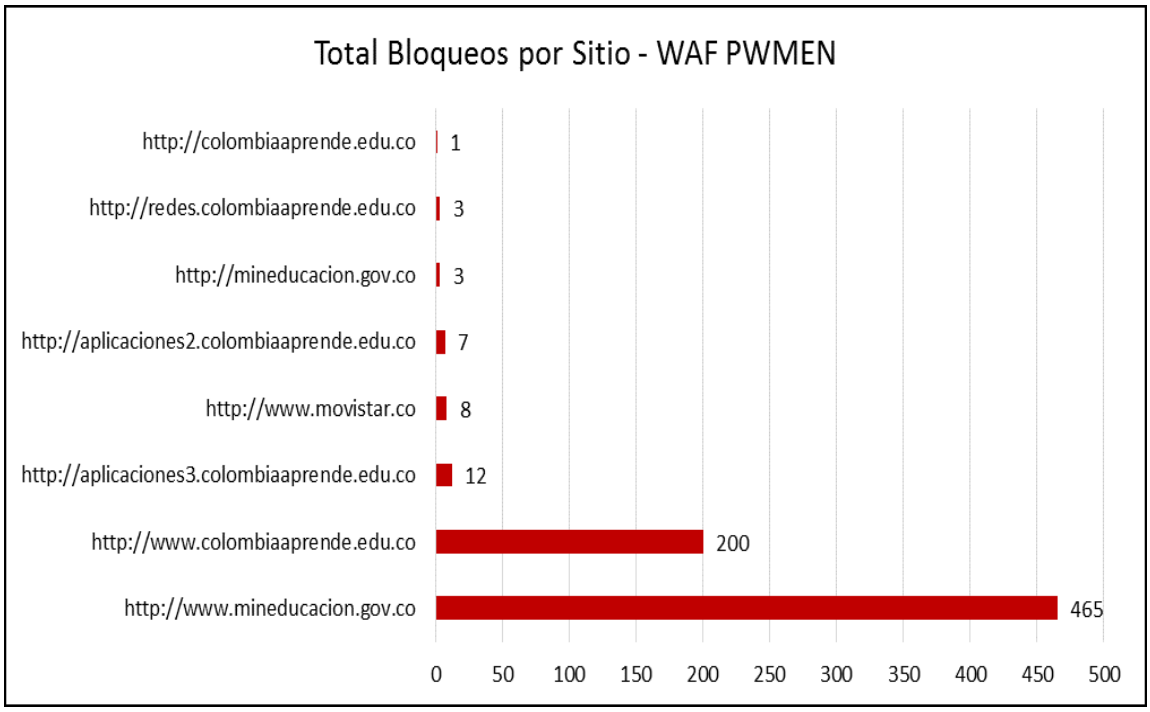


Fuente: Logs WAF mes de diciembre 2016.

Las 3 firmas con mayor número de bloqueos identificadas como amenazas son: “web-misc squid authentication headers handling denial of service attempt, web-misc /.... access y web-client corehttp long buffer overflow attempt " con el 97%, 1.29% y 1% respectivamente del total de eventos bloqueados.

- **Top bloqueo por sitios**

Gráfica 102. Bloqueo por sitio WAF – diciembre 2016



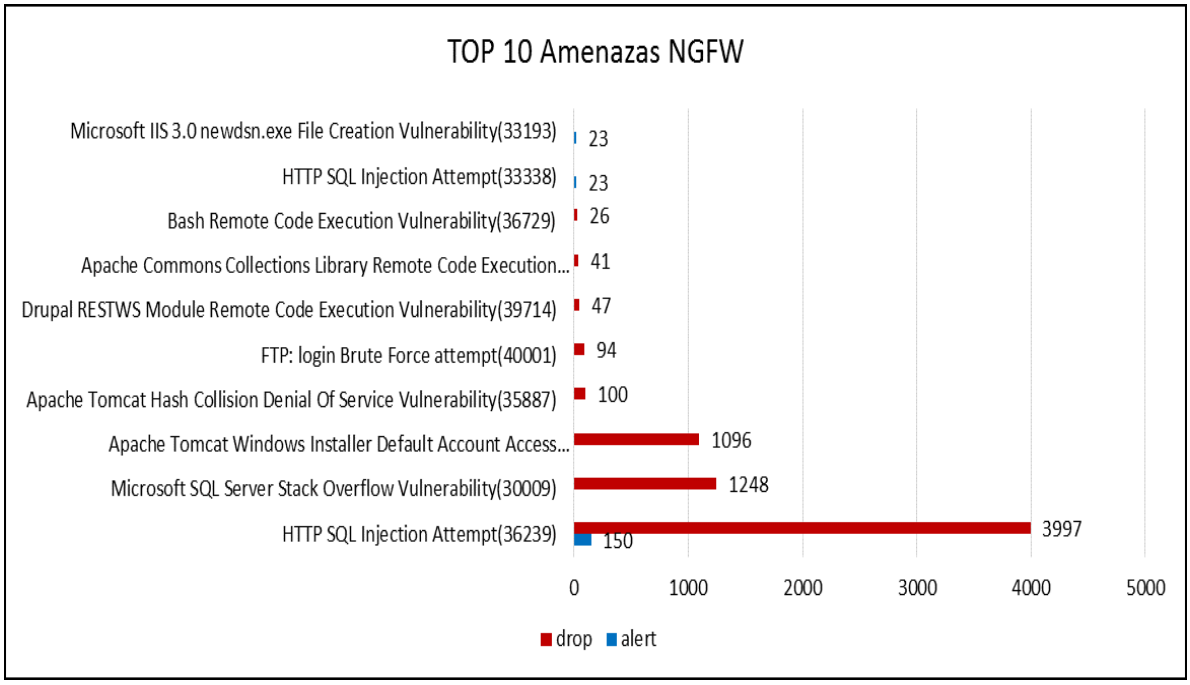
Fuente: Logs WAF mes de diciembre 2016.

Como se observa en la gráfica 102, los 3 sitios web con mayor número de firmas bloqueadas identificadas como amenazas son: *"www.mineducacion.gov.co"* con el 66.5%, *"www.colombiaaprende.edu.co"* con el 28.6% y *"aplicaciones3.colombiaaprende.edu.co"* con el 1.7% del total de firmas bloqueadas.

CAN NGFW

- **Top de amenazas por firma**

Gráfica 103. Top 10 amenazas NGFW CAN - diciembre 2016

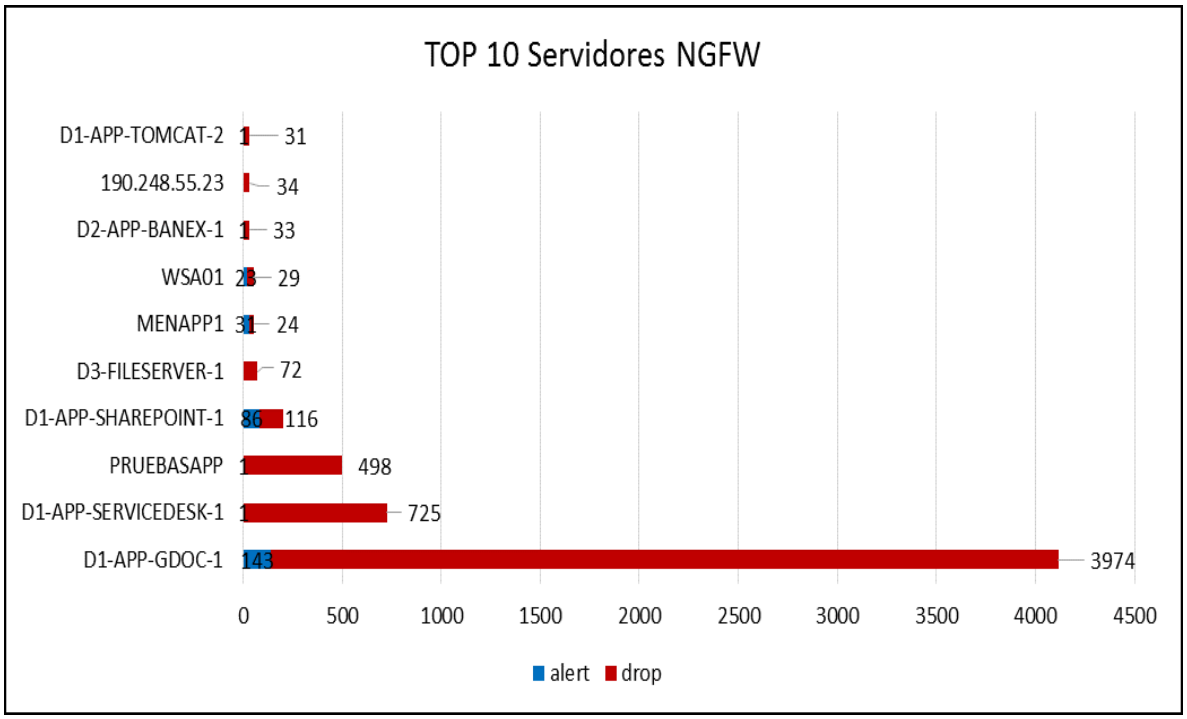


Fuente: Logs NGFW CAN mes de diciembre 2016.

Como se observa en la gráfica 103, las 3 firmas con mayor número de eventos son: *"HTTP SQL Injection Attempt (36239), Microsoft SQL Server Stack Overflow Vulnerability (30009) y Apache Tomcat Windows Installer Default Account Access Vulnerability (34160)"*, con el 58,42%, 17,58% y 15,44% respectivamente del total de eventos detectados, donde las barras azules representan los eventos permitidos y las barras de color rojo los eventos bloqueados catalogados como amenazas.

- **Top de servidores con más eventos**

Gráfica 104. Top servidores con más eventos NGFW CAN - diciembre 2016

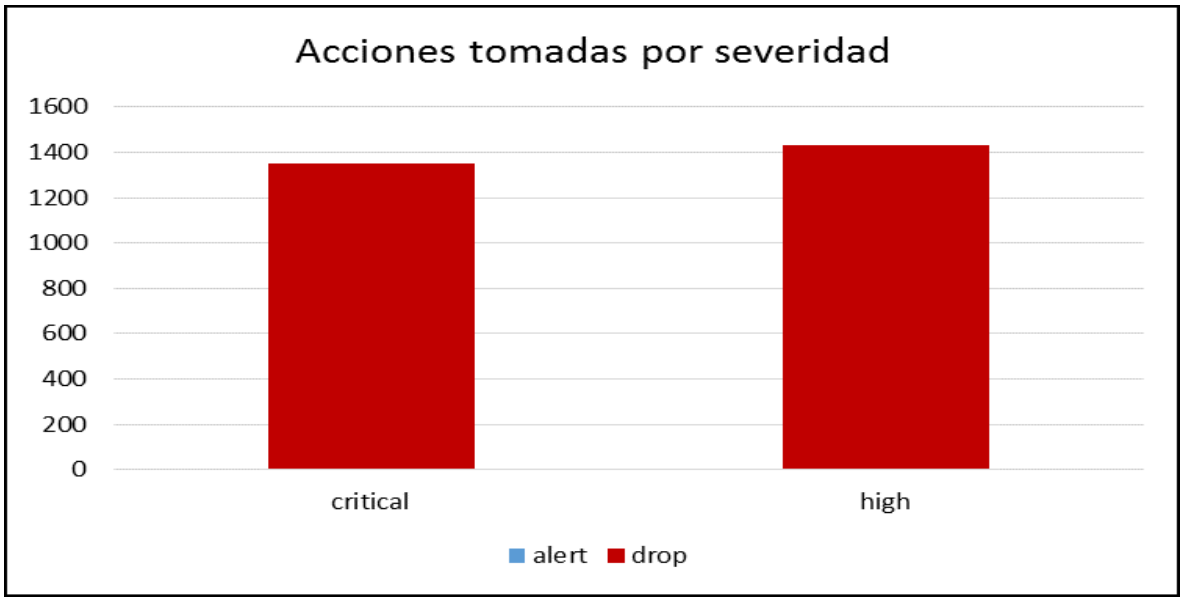


Fuente: Logs NGFW CAN mes de diciembre 2016.

Como se observa en la gráfica 104, los 3 servidores con mayor número de eventos son: *"D1-APP-GDOC-1"* con el 58%, *"D1-APP-SERVICEDESK-1"* con el 10.2% y *"PRUEBASAPP"* con el 7% del total de eventos detectados, donde las barras azules representan las firmas permitidas y las barras de color rojo las firmas bloqueadas identificadas como amenazas.

- **Acciones por severidad *critical* y *high***

Gráfica 105. Acciones tomadas por severidad NGFW CAN - diciembre 2016



Fuente: Logs NGFW CAN mes de diciembre 2016.

Como se observa en la gráfica 105, el 100% de las amenazas con severidades *critical* y *high* están siendo bloqueadas en el NGFW de la sede del CAN.

- **Anti-Virus**

Cuadro 31. Eventos de anti-virus registrado en el NGFW CAN – diciembre 2016

Firma virus	Eventos
Trojan/Win32.docdl.bvb (1210068)	14
Worm/Win32.allaple.vttlg (2318491)	5
Virus/Win32.fusioncore.a (2407177)	4
TrojanDownloader/O97M.donoff.cpg (1200405)	3
Virus/Android.WGeneric.kqyoa (1009052)	2
Virus/RDN.adwind.bd (1252140)	2
Virus/Win32.WGeneric.eeint (1270109)	2
Virus/Android.WGeneric.kixwk (1003241)	1
Virus/Win32.slugin.qto (2043442)	1
Virus/Win32.WGeneric.kquxp (1200545)	1
Total	**35**

Fuente: Logs NGFW CAN mes de diciembre 2016.

El 100% de las firmas detectadas por el módulo de anti-virus que se observan en el cuadro 31 fueron bloqueadas.

- **Anti-Spyware**

Cuadro 32. Eventos de anti-spyware registrado en el NGFW CAN – diciembre 2016

Firma spyware	Eventos
Sipvicious.Gen User-Agent Traffic (13272)	90079
Suspicious DNS Query (generic:port.e5555sk5yws55sk.com) (4002719)	7869
Suspicious DNS Query (generic:www.sedchoco.gov.co) (4017193)	139
Suspicious DNS Query (generic:www.fods-apple.com) (4034540)	134
Suspicious DNS Query (generic:763d.dl.filesearcher.biz) (4069476)	85
Suspicious DNS Query (generic:zglsdzm.unitnightcome.ru) (4002133)	50
Win32.Conficker.C p2p (12544)	44
Suspicious DNS Query (generic:kepjxengluqnmymhj.pro) (4069235)	43
Suspicious DNS Query (generic:qbkipiodeojnbosilo.pro) (4070670)	43
Suspicious DNS Query (generic:iuffawjutkswcqbysyt.pro) (4072296)	42
Total	**99489**[61]
Fuente: Logs NGFW CAN mes de diciembre 2016.	

Las 3 firmas de anti-spyware con mayor número de eventos, de acuerdo al cuadro 32 son: *"Sipvicious.Gen User-Agent Traffic (13272), Suspicious DNS Query (generic: port.e5555sk5yws55sk.com) (4002719) y Suspicious DNS Query (generic: www.sedchoco.gov.co) (4017193)"*, con el 73.3%, 16.6% y 8.2% respectivamente del total de spyware detectado.

El 70.3% de eventos detectados dentro de esta categoría fueron bloqueados luego de que se aplicara la política de bloqueo de firmas con severidades *critical*, high, médium y *low* en la sede del CAN. Los eventos que no se bloquean son clasificados con severidad *informative*.

[61]El total refleja la suma de todos los eventos asociados a las firmas de esta categoría y no solamente los mostrados en el TOP 10.

- **Eventos WildFire**

Cuadro 33. Eventos de Wildfire registrado en l el NGFW CAN – diciembre 2016

Servidor	Microsoft MS office (52033)	Microsoft PE file (52060)	Windows executable (EXE) (52020)	Total general
190.248.55.2	-	-	42	42
190.248.55.21	13	4	10	27
Total general	**13**	**4**	**52**	**69**

Fuente: Logs NGFW CAN mes de diciembre 2016.

Los archivos revisados por el sistema Wildfire, que se observan en el cuadro 33, son objetos con probabilidad de ser maliciosos, que son ejecutados y analizados en un entorno controlado. El sistema Wildfire realiza un diagnóstico, en donde si los archivos recientemente analizados se consideran maliciosos, se genera el reporte y se alimenta el repositorio de Palo Alto.

El 60,8% de los eventos diagnosticados por la nube de Palo Alto como "*malware*" tenían como destino la IP pública 190.248.55.21, lo que indica que corresponden a correos electrónicos con archivos ejecutables de carácter malicioso.

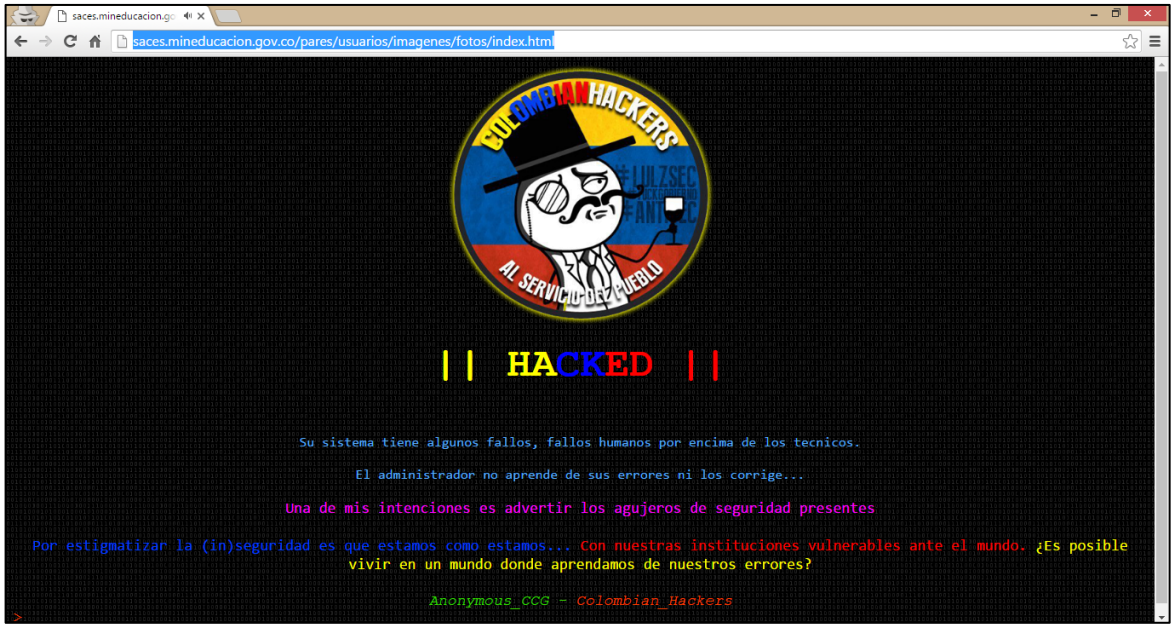
ANEXO D. INCIDENTES DE SEGURIDAD

Website Defacement - 8 de junio de 2016

El día 8 de junio de 2016, el equipo de seguridad informática de manera proactiva identificó incidente de seguridad relacionado con la carga no autorizada de archivos en el sitio web en el sitio web de SACES - PARES perteneciente al MEN, como se observa en la gráfica 106.

- http://saces.mineducacion.gov.co/pares/usuarios/imagenes/fotos/index.html

Gráfica 106. *Defacement* página SACES – PARES



Fuente: acceso el 8 de junio de 2016 página web: http://saces.mineducacion.gov.co/pares/usuarios/imagenes/fotos/index.html

Una vez realizada la verificación y confirmación del incidente, se procedió a fijar en sitio web afectado en modo “mantenimiento” a través de un “*redirect*”, como se observa en la gráfica 107.

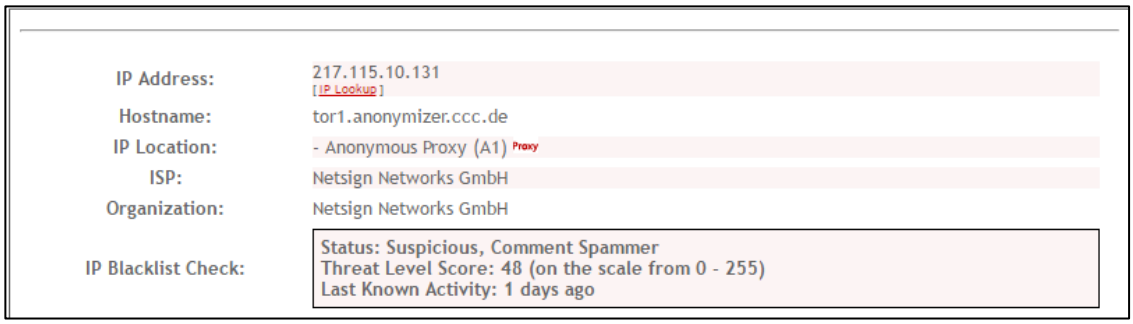
Gráfica 107. Página en mantenimiento para el acceso a SACES – PARES

Fuente: acceso el 8 de junio de 2016 página web: http://saces.mineducacion.gov.co/pares/usuarios/imagenes/fotos/index.html

Una vez controlado el incidente, se procedió a validar sobre la ruta raíz y subcarpetas, revisión de logs en el servidor, validar permisos y privilegios sobre las carpetas, adicionalmente se revisaron los puntos de entrada sobre la página web para la realización de la carga no autorizada, se omiten estas evidencias (pantallazos) porque no son objetivo de este proyecto de investigación.

En los logs del servidor se identificó la IP origen del ataque atacante, donde se observa en la gráfica 108 que la IP detectada tiene como localización "*Anonymous proxy*", lo cual oculta el verdadero origen.

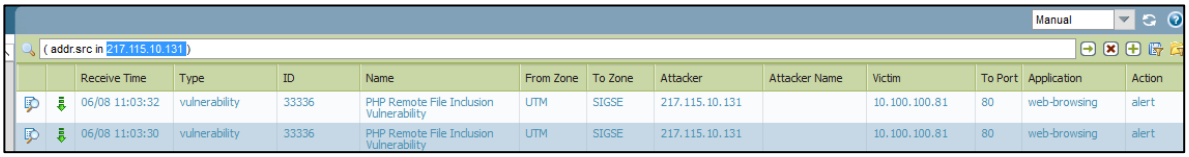
Gráfica 108. Identificación de la IP por Geolocalización



Fuente: Identificación web de la IP por Geolocalización.

Adicionalmente se llevó a cabo una revisión de los registros generados por los dispositivos de seguridad NGFW y WAF, identificando que alrededor de la hora en que fueron creados los directorios en el servidor, los registros de vulnerabilidad relacionada con *PHP Remote File Inclusion Vulnerability* (33336) con severidad *medium*, el cual se estaba ejecutando la acción de *alert*, como se puede observar en la figura 31.

Figura 31. Identificación de la firma PHP Remote File Inclusion Vulnerability en el módulo de amenazas del NGFW – DIVEO



Fuente: Logs NGFW DIVEO el 8 de junio de 2016.

Ésta vulnerabilidad PHP Remote File Inclusion Vulnerability (33336) con severidad *medium* indica: "*Múltiple PHP products are prone to a remote file inclusion vulnerability while parsing certain crafted HTTP response. The vulnerability is due to the lack of proper checks in the HTTP response, leading to an exploitable remote file inclusion. An attacker could exploit the vulnerability by sending a crafted HTTP response. A successful attack could lead to remote code execution with the privileges of the server*"[62].

En el dispositivo WAF no identifico ninguna firma relacionada con el incidente.

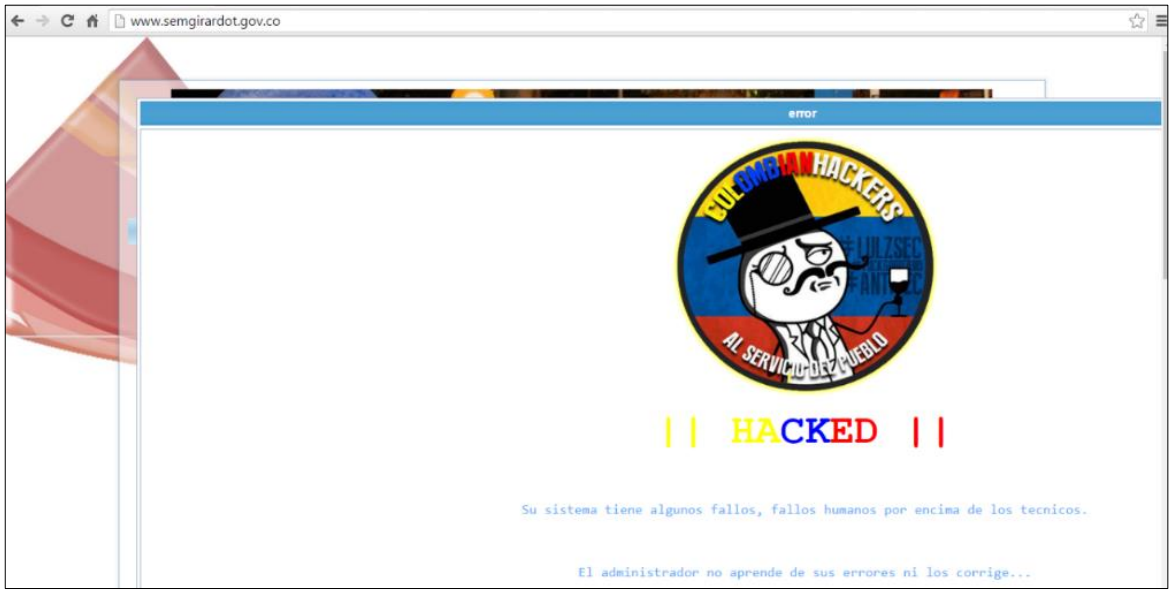
[62] PALO ALTO NETWORK. THREAT VAULT. [En línea], [consultado el 10 de junio de 2016]. Disponible en: https://threatvault.paloaltonetworks.com/

***Website Defacement* - 22 de Julio de 2016**

El día 22 de Julio de 2016, el equipo de seguridad informática de manera proactiva identificó incidente de seguridad relacionado con la carga no autorizada de archivos en el sitio web de la Secretaría de Educación Municipal de Girardot perteneciente al MEN, como se observa en la gráfica 109.

- http://www.semgirardot.gov.co/

Gráfica 109. *Defacement* página SEMGIRARDOT



Fuente: acceso el 22 de Julio de 2016 página web: http://saces.mineducacion.gov.co/pares/usuarios/imagenes/fotos/index.html

Una vez realizada la verificación y confirmación del incidente, se procedió a fijar en sitio web afectado en modo “mantenimiento” a través de un “*redirect*”, como se observa en la gráfica 110.

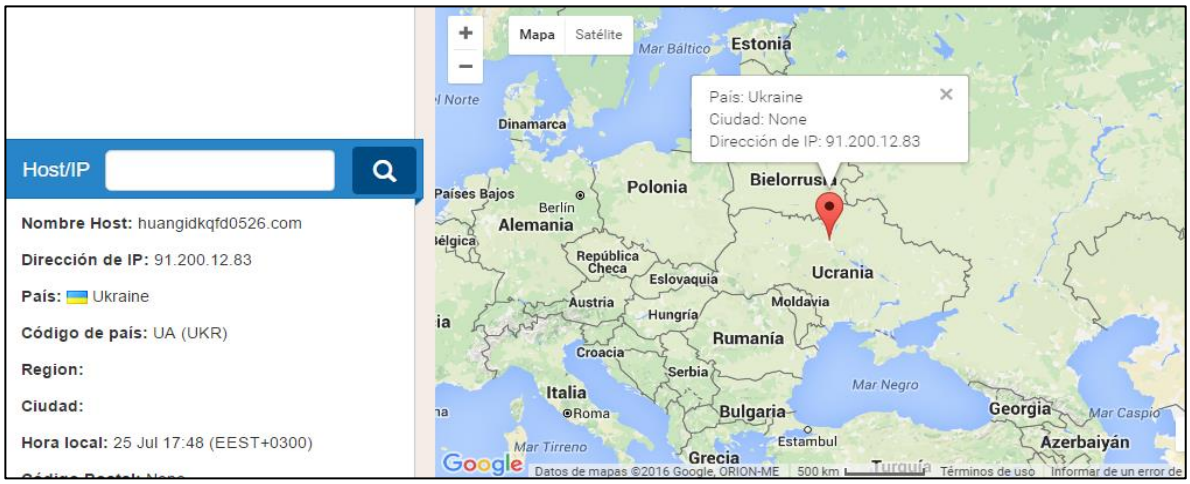
Gráfica 110. Página en mantenimiento para el acceso a SEMGIRARDOT

Fuente: acceso el 22 de Julio de 2016 página web: http://saces.mineducacion.gov.co/pares/usuarios/imagenes/fotos/index.html

Una vez controlado el incidente, se procedió validar sobre la ruta raíz y subcarpetas, revisión de logs en el servidor, validar permisos y privilegios sobre las carpetas, adicionalmente se revisaron sobre la página web los puntos de entrada para la realización de la carga no autorizada, se omiten estas evidencias (pantallazos) porque no son objetivo de este proyecto de investigación.

En los logs del servidor se identificó la IP origen del ataque correspondiente al país de Ucrania, como se observa en la gráfica 111.

Gráfica 111. Identificación de la IP por Geolocalización

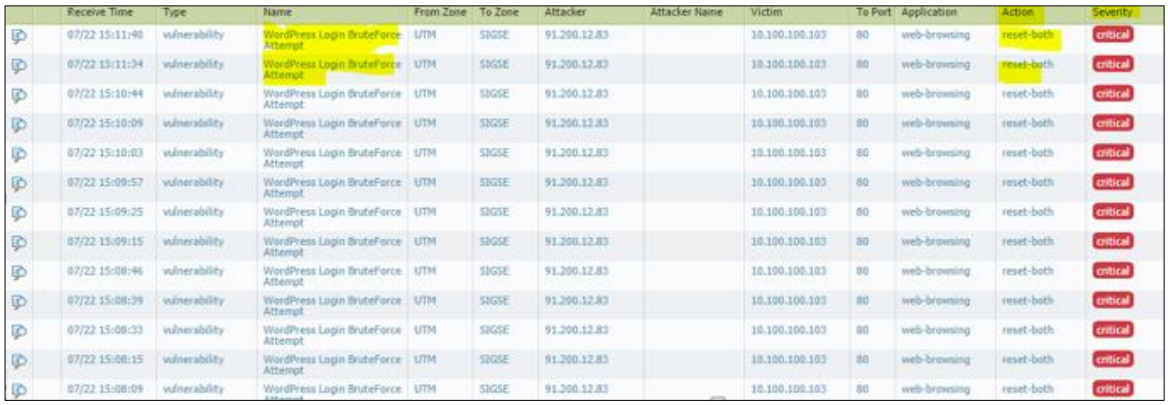


Fuente: Identificación web de la IP por Geolocalización.

Posteriormente a la identificación IP del atacante se procede a revisar y analizar los logs de los dispositivos de NGFW y WAF de DIVEO encontrando lo siguiente:

Para la validación en los NGFW se realiza un filtro en el módulo de amenazas con la IP Origen de Ucrania 91.200.12.83, donde se observa que la IP del atacante está catalogado únicamente con severidad *critical*, la firma se llama *WordPress Login BruteForce Attempt* (40044) con severidad *critical*, la cual se encuentra bloqueada, como se observa en la figura 32.

Figura 32. Identificación de la firma *WordPress Login BruteForce Attempt* en el módulo de amenazas del NGFW – DIVEO



Receive Time	Type	Name	From Zone	To Zone	Attacker	Attacker Name	Victim	To Port	Application	Action	Severity
07/22 15:11:40	vulnerability	WordPress Login BruteForce Attempt	UTM	SIGSE	91.200.12.83		10.100.100.103	80	web-browsing	reset-both	critical
07/22 15:11:34	vulnerability	WordPress Login BruteForce Attempt	UTM	SIGSE	91.200.12.83		10.100.100.103	80	web-browsing	reset-both	critical
07/22 15:10:44	vulnerability	WordPress Login BruteForce Attempt	UTM	SIGSE	91.200.12.83		10.100.100.103	80	web-browsing	reset-both	critical
07/22 15:10:09	vulnerability	WordPress Login BruteForce Attempt	UTM	SIGSE	91.200.12.83		10.100.100.103	80	web-browsing	reset-both	critical
07/22 15:10:03	vulnerability	WordPress Login BruteForce Attempt	UTM	SIGSE	91.200.12.83		10.100.100.103	80	web-browsing	reset-both	critical
07/22 15:09:57	vulnerability	WordPress Login BruteForce Attempt	UTM	SIGSE	91.200.12.83		10.100.100.103	80	web-browsing	reset-both	critical
07/22 15:09:25	vulnerability	WordPress Login BruteForce Attempt	UTM	SIGSE	91.200.12.83		10.100.100.103	80	web-browsing	reset-both	critical
07/22 15:09:15	vulnerability	WordPress Login BruteForce Attempt	UTM	SIGSE	91.200.12.83		10.100.100.103	80	web-browsing	reset-both	critical
07/22 15:08:46	vulnerability	WordPress Login BruteForce Attempt	UTM	SIGSE	91.200.12.83		10.100.100.103	80	web-browsing	reset-both	critical
07/22 15:08:39	vulnerability	WordPress Login BruteForce Attempt	UTM	SIGSE	91.200.12.83		10.100.100.103	80	web-browsing	reset-both	critical
07/22 15:08:33	vulnerability	WordPress Login BruteForce Attempt	UTM	SIGSE	91.200.12.83		10.100.100.103	80	web-browsing	reset-both	critical
07/22 15:08:15	vulnerability	WordPress Login BruteForce Attempt	UTM	SIGSE	91.200.12.83		10.100.100.103	80	web-browsing	reset-both	critical
07/22 15:08:09	vulnerability	WordPress Login BruteForce	UTM	SIGSE	91.200.12.83		10.100.100.103	80	web-browsing	reset-both	critical

Fuente: Logs NGFW DIVEO el 22 de Julio de 2016.

La firma denominada WordPress Login BruteForce Attempt (40044) con severidad *critical* indica: "*This event indicates that someone is using a brute force attack to gain access to WordPress wp-login.php. The brute force signature looks for (by default) 10 or more triggers of child signature TID: 37480 in 60 seconds. The child signature is looking for access attempts to wp-login.php*"[63].

Luego se revisar el módulo de amenazas, se procede a revisar el módulo de tráfico realizando el mismo filtro de IP origen donde se puede observar el tráfico permitido la IP de Ucrania 91.200.12.83, la acción es permitir todo y el tamaño del paquete es el mismo 1.9 KB donde se considera que está accediendo realizando pruebas reiterativas de *login,* pero manteniendo la misma longitud de credenciales como se observa en la figura 33.

[63] PALO ALTO NETWORK. THREAT VAULT. [En línea], [consultado el 24 de Julio de 2016]. Disponible en: https://threatvault.paloaltonetworks.com/

Figura 33. Identificación de la firma *WordPress Login BruteForce Attempt* en el módulo de tráfico del NGFW – DIVEO

	Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action	Rule	Session End Reason	Bytes
	07/22 15:10:56	end	UTM	SIGSE	91.200.12.83		10.100.100.103	80	web-browsing	allow	Permitir todo	tcp-rst-from-client	1.9k
	07/22 15:10:55	end	UTM	SIGSE	91.200.12.83		10.100.100.103	80	web-browsing	allow	Permitir todo	tcp-rst-from-client	1.9k
	07/22 15:10:55	end	UTM	SIGSE	91.200.12.83		10.100.100.103	80	web-browsing	allow	Permitir todo	tcp-rst-from-client	1.9k
	07/22 15:10:54	end	UTM	SIGSE	91.200.12.83		10.100.100.103	80	web-browsing	allow	Permitir todo	tcp-rst-from-client	1.9k
	07/22 15:10:53	end	UTM	SIGSE	91.200.12.83		10.100.100.103	80	web-browsing	allow	Permitir todo	tcp-rst-from-client	1.9k
	07/22 15:10:53	end	UTM	SIGSE	91.200.12.83		10.100.100.103	80	web-browsing	allow	Permitir todo	tcp-rst-from-client	1.9k
	07/22 15:10:53	end	UTM	SIGSE	91.200.12.83		10.100.100.103	80	web-browsing	allow	Permitir todo	tcp-rst-from-client	1.9k
	07/22 15:10:52	end	UTM	SIGSE	91.200.12.83		10.100.100.103	80	web-browsing	allow	Permitir todo	tcp-rst-from-client	1.9k
	07/22 15:10:52	end	UTM	SIGSE	91.200.12.83		10.100.100.103	80	web-browsing	allow	Permitir todo	tcp-rst-from-client	1.9k

Fuente: Logs NGFW DIVEO el 22 de Julio de 2016.

En el dispositivo WAF no identifico ninguna firma relacionada con el incidente.