POR UN DESARROLLO SOSTENIBLE
FOR A SUSTAINABLE DEVELOPMENT
Informática
XVII CONVENCIÓN Y FERIA INTERNACIONAL 17TH INTERNATIONAL CONVENTION AND FAIR 2018
La Habana, Cuba. Del 19 al 23 de marzo
Havana, Cuba. March 19th to 23th

CLEANING CENTER. UN NUEVO SERVICIO DE ETECSA
CLEANING CENTER. A NEW ETECSA SERVICE

Ing. Javier Brooks Miranda[1], Lic. Michel Rodríguez Averoff[2]

1 ETECSA, javier.brooks@etecsa.cu, 10200

2 ETECSA, michel.everoff@etecsa.cu

RESUMEN: *Con el fin de garantizar la ciberseguridad aparejado con la creciente demanda de servicios de acceso a internet en la que está inmersa la Empresa de Telecomunicaciones de Cuba S.A (ETECSA), el Departamento de Seguridad de Redes de la Dirección de Operaciones de Seguridad diseña e implementa una plataforma para el análisis, monitoreo y control del tráfico malicioso en los puntos de presencia de los servicios de acceso a internet (PoP de Servicio). Los resultados y experiencias obtenidas durante la explotación de esta plataforma han sido el precedente del Cleaning Center: un nuevo servicio que ofrecerá ETECSA, el cual permitirá a las empresas emplear una protección sobre su red sin necesidad de comprar ni desplegar costosas soluciones de hardware y software en sus instalaciones.*

El Cleaning Center está diseñado como parte del servicio de acceso a Internet, de forma que la protección frente ataques, programas malignos, fuentes maliciosas, entre otros, sea su característica esencial. Con este servicio, las empresas obtendrán una protección completa de acceso a internet y un análisis detallado de los eventos de seguridad asociados a sus redes de servicios. Diseñado para facilitar el trabajo del analista de seguridad, el Cleaning Center proveerá a las entidades cuadros de mandos que ofrezcan una panorámica de las principales amenazas. El Cleaning Center será un servicio integrado a los que hoy se brindan y permitirá el control del tráfico de la red ante las amenazas actuales y futuras como parte del proceso de mitigación de riesgos presente en la gestión de incidentes de seguridad informática en cualquier empresa.

Palabras Clave: *Amenazas, Seguridad, Monitoreo, Control, Tráfico*

ABSTRACT: *In order to guarantee cybersecurity coupled with the growing demand for Internet access services in which the Telecommunications Company of Cuba S.A (ETECSA) is immersed, the Department of Network Security of the Security Operations Directorate designs and implements a platform for the analysis, monitoring and control of malicious traffic in the points of presence of Internet access services (Service PoP). The results and experiences obtained during the exploitation of this platform have been the precedent of the Cleaning Center: a new service offered by ETECSA, which will allow companies to use protection over their network without having to buy or deploy expensive hardware and software solutions in its facilities.*

The Cleaning Center is designed as part of the Internet access service, so that protection against attacks, malign programs, malicious sources, among others, is its essential characteristic. With this service, companies will obtain complete protection of Internet access and a detailed analysis of the security events associated with their service networks. Designed to facilitate the work of the security analyst, the Cleaning Center will provide the entities with control panels that offer an overview of the main threats. The Cleaning Center will be an integrated service to those currently offered and will allow the control of network traffic in the face of current and future threats as part of the risk mitigation process present in the management of computer security incidents in any company.

KeyWords: *Threats, Security, Monitoring, Control, Traffic*

1. INTRODUCCIÓN

El monitoreo de seguridad en las redes de servicio de acceso a internet se hace necesario en todo tipo de empresas debido a las demandas en las exigencias de las operaciones y la complejidad en sus redes de cómputo. El análisis, monitoreo y control de tráfico toma mayor importancia y debe tener un carácter pro-activo, con el fin de evitar problemas a futuro.

La Plataforma de Monitoreo y Control del Tráfico Malicioso (PMCTM) en las redes de servicio, constituyen el soporte tecnológico fundamental para el cumplimiento de la misión y funciones de cualquier Centro de Operaciones de Seguridad (COS): "realizar el monitoreo continuo del estado de la seguridad informática, la detección oportuna de las amenazas, ataques e incidentes de seguridad relacionados con estas y la gestión de la respuesta ante las mismas".

1.1 Antecedentes y problemática

En marzo de 2014 se realizan ataques de desconfiguración de servicios a usuarios y entidades nacionales con acceso a los servicios de Internet. Como parte de la investigación de estos incidentes de seguridad ocurridos, se evidenció la falta de visibilidad del tráfico malicioso en nuestras redes y la necesidad de disponer de un sistema para el monitoreo de dicho tráfico.

Un mes más tarde, se toma la decisión de realizar un monitoreo del tráfico malicioso que constituyó el primer paso de un programa de trabajo para el desarrollo de un sistema de inteligencia de amenazas, que permitiera identificar indicadores de compromiso. Se desplegó un sensor con el IDS (Sistema de Detección de Intrusos) Suricata, al que se le hizo llegar, a través de la red privada de seguridad de la DOPS, el tráfico de puertos espejos de los diferentes Puntos de Presencia de los Servicios(PoP). Simultáneamente se añadieron el conjunto de reglas ETPro (Emerging Threat Professional Ruleset), las cuales se actualizan sistemáticamente, para la detección de amenazas con el este IDS.

En ese mismo año, los servicios de navegación con tecnología Wifi se trataron de expandir a las salas de navegación. Las necesidades de prestar dichos servicios a la población en espacios públicos y con un carácter extensivo hicieron que se modificarán algunas de las premisas iniciales expandiendo la posición no solo a las salas de navegación sino también a sitios de alta concentración de usuarios en los espacios públicos del país.

La necesidad de la proyección de un sistema de comunicaciones que posibilite el acceso inalámbrico a Internet en diferentes puntos del país, así como el despliegue de un conjunto de subsistemas que apoyen la operación; hace que ETECSA expanda el Proyecto WLAN con tecnología Wi-Fi. La necesidad de ETECSA de desplegar estos servicios con la mayor rapidez posible, hizo necesario proponer una plataforma de monitoreo y control de tráfico para la detección y mitigación de amenazas e incidentes de seguridad.

En enero del 2015 se le asigna al COS la responsabilidad de conceptualizar los controles de ciberseguridad necesarios para el servicio WLAN que la empresa estaba persiguiendo poner en marcha y que carecía de las funcionalidades que dieran cumplimiento a los requerimientos de la Dirección de Operaciones de Seguridad de ETECSA (DOPS).

Seis meses más tarde el servicio WLAN se comienza a brindar con esta plataforma. Con el transcurso del tiempo, esta primera solución resulto ineficiente teniendo en cuenta el crecimiento del tráfico maliciosos a monitorear y controlar, en correspondencia con la ampliación de dichos servicios, por lo cual se ha ido mejorando y constituye una tarea permanente del COS.

Para el lanzamiento del servicio WLAN, se adquirieron recursos de hardware para comenzar la implementación de un sistema para el monitoreo del tráfico malicioso asociado a dicho servicio. Adicionalmente se conceptualizó y ejecutó una solución de control de tráfico no deseado, basado en software libre (pFsense y Suricata), conocida como Mambí1.0 para cumplir requerimientos de seguridad establecidos para este servicio. Esta solución a largo plazo se vería afectada por el creciente nivel de tráfico producto del aumento de ancho de banda que se ofrece para brindar una mejor calidad de servicio. Se pudo comprobar que a partir de un tráfico mayor de 1.5 Gbps esta solución (pFsense) presentaba perdidas de paquetes a procesar.

Para suplir esta deficiencia y que el servicio se siguiera ofreciendo con el nivel de seguridad requerido, se implementa el Mambí2.0. Esta versión está basada en un IDS Suricata con la funcionalidad de IPS (Sistema de Prevención de Intrusos) lo cual permite continuar con las características propias del firewall pFsense de la solución anterior en cuanto a bloqueo de paquetes y posibilita además trabajar

con tráficos de hasta 10 Gbps. Esta solución que está integrada con herramientas como NETDATA y Grafana para la visualización de los datos de interés (tráfico, paquetes bloqueados, rendimiento de RAM y CPU, etc.), fue implementada en los PoP y hoy en día es la encargada del control del tráfico malicioso en estos puntos. Además, está perfectamente integrada con el stack de Elastic (ELK, Elasticsearch-Logstash-Kibana) para la visualización de los eventos y alertas de seguridad detectados.

La PMCTM garantiza un nivel de seguridad en el monitoreo y control del tráfico malicioso actualmente en explotación en redes de servicio Nauta y de acceso Wifi en espacios públicos, así como los nuevos servicios ADSL Hogar y el acceso a Internet desde redes móviles (3G).

2. CONTENIDO

Cuando hablamos de amenazas, según [1], nos referimos a aquellos cambios del entorno por parte de un humano, una máquina o simplemente, un suceso que pueda comprometer la seguridad de determinada empresa. Las amenazas pueden ser detectadas antes, después o durante el ataque. Para ello, las intervenciones posibles son:

- Prevención: se trata de mecanismos que ayudan a mejorar la seguridad en un funcionamiento rutinario.
- Detección: dispositivos encargados de revelar posibles violaciones de las políticas de seguridad.
- Recuperación: mecanismos preparados para activarse cuando se produce un ataque y restaurarlo a su estado de funcionamiento normal.

Según las amenazas, podemos clasificarlas según:

- Origen:
  - Amenazas Internas: pueden ser causadas por un uso incorrecto por parte de la plantilla o por personal técnico, que, por motivos de necesidad en el trabajo, tienen acceso a partes críticas de la red. Los sistemas de prevención contra intrusiones o los cortafuegos, no son eficientes contra amenazas internas, ya que no están guiados al tráfico interno.
  - Amenazas Externas: son aquellas que proceden del exterior. No se tiene información evidente sobre la red y los atacantes deben primero entender cómo funciona para luego buscar una manera para asaltarla. El analista de seguridad, tiene la oportunidad de prevenir de manera correcta este tipo de ataques.
- Efecto:
  - Estafa, Robo de dinero
  - Suplantación de identidad
  - Publicidad de datos personales
  - DDOS de los sistemas
  - Destrucción de información confidencial
- Medio:
  - Virus: malware que intenta alterar la actividad normal del dispositivo, sin el consentimiento del usuario.
  - Phising
  - Ingeniería Social
  - DDOS Spoofing

Las plataformas de seguridad actualmente en una empresa están en constate cambio y desarrollo. ETECSA como principal proveedor de servicios tiene el deber, el compromiso y la misión de brindar servicios de telecomunicaciones que satisfagan las necesidades de los clientes y la población. Por tanto, los sistemas de análisis, monitoreo y control de tráfico, están en contaste perfeccionamiento atendiendo a los requerimientos a la hora de ofrecer un determinado servicio. A continuación, se presentan un conjunto de herramientas utilizadas para llevar a cabo el control del tráfico malicioso en los puntos de presencia de los servicios de acceso a internet, las cuales constituyen la base del Cleaning Center.

2.1 Suricata

Suricata es un motor de detección de amenazas gratuita de código abierto, una herramienta madura, rápida y sólida. Está preparado para detección de intrusión en tiempo real (IDS), prevención de intrusiones en línea (IPS), monitoreo de seguridad de red (NSM) y procesamiento de ficheros pcap sin conexión.

Suricata inspecciona el tráfico de la red utilizando potentes y extensas reglas y lenguaje de firmas, y tiene un poderoso soporte de secuencias de comandos Lua[1] para la detección de amenazas complejas. Con formatos estándar de entrada y salida como YAML y JSON, se vuelven fáciles las integraciones con herramientas existentes como los SIEM, Splunk, Logstash/Elasticsearch, Kibana y otras bases de datos.
El desarrollo de Suricata impulsado por la comunidad a un ritmo acelerado se centra en la seguridad, la usabilidad y la eficiencia. El proyecto y el código de este IDS-IPS es propiedad y está respaldado por Open Information Security Foundation (OISF), una fundación sin fines de lucro comprometida con asegurar el desarrollo de Suricata y el éxito sostenido como una herramienta de código abierto.[2]

[1] Lua es un lenguaje de programación extensible diseñado para una programación procedimental general con utilidades para la descripción de datos. También ofrece un buen soporte para la programación orientada a objetos, programación funcional y programación orientada a datos.

2.1.1 Características

Suricata implementa un completo lenguaje de firmas para la correlación con amenazas conocidas, violación de políticas y comportamiento malicioso. Detecta muchas anomalías en el tráfico que inspecciona y utiliza el conjunto de reglas especializadas Emerging Threats y el conjunto de reglas VRT[2].

Alto rendimiento: Una sola instancia de Suricata es capaz de inspeccionar el tráfico de varios gigabits. El motor está construido alrededor de una base de código multihilo, moderna y altamente escalable. Existe compatibilidad nativa para la aceleración de hardware de varios proveedores a través de PF_RING y AF_PACKET.

Detección automática de protocolo: Suricata detectará automáticamente protocolos como HTTP en cualquier puerto y aplicará la lógica adecuada de detección y registro, ayudando enormemente a la localización de programas malignos y dominios C&C[3].

NSM (más que un IDS): También puede inspeccionar solicitudes HTTP, registrar y almacenar certificados TLS, extraer archivos de flujos y almacenarlos en el disco. Soporta de capturas completas de pcap que permite un análisis sencillo. Todo esto hace que Suricata sea un poderoso motor para su ecosistema de Monitoreo de Seguridad de Red (NSM).

- Registro y análisis TLS / SSL: no solo puede coincidir con los aspectos de un intercambio SSL/TLS dentro del conjunto de reglas gracias al TLS Parser de Suricata, también puede registrar todos los intercambios de claves para su análisis. Una excelente manera de asegurarse de que su red no sea víctima de una autoridad certificadora menos confiable.
- Registro HTTP: ¿Por qué agregar más hardware a su red solo para registrar la actividad http cuando su IDS ya la ve? Suricata registrará todas las conexiones HTTP en cualquier puerto para su posterior análisis.[3]

La arquitectura de múltiples hilos de Suricata es única, ya que puede soportar sistemas multi-núcleo y multiprocesador de alto rendimiento. Los principales beneficios de un diseño de múltiples hilos es que ofrece mayor velocidad y eficiencia en el análisis de tráfico de red y también puede ayudar a dividir la carga de trabajo de IDS / IPS en función de las necesidades de procesamiento. Además de la aceleración de hardware (con limitaciones de hardware y de tarjeta de red), el motor está diseñado para utilizar la mayor potencia de procesamiento ofrecida por los últimos chips de CPU multi-núcleo. Suricata se ha desarrollado con la idea de una fácil implementación, acompañado de documentación de inicio paso-a-paso y un potente manual de usuario. El motor también ha sido desarrollado en C, pensado desde los inicios para escalar. Adicionalmente, para facilitar la migración a este producto, Suricata emplea las mismas reglas y formatos de salida que Snort.[4]

2.2 ELK

Al combinar las herramientas masivamente populares Elasticsearch, Logstash y Kibana (lo que se conoce como Elastic Stack o ELK), Elastic ha creado una plataforma extremo a extremo que ofrece información procesable en tiempo real de casi cualquier tipo de fuente de datos estructurados y no estructurados. Construido y respaldado por ingenieros detrás de cada uno de estos productos de código abierto, Elastic Stack hace que las búsquedas y el análisis de datos sea más fácil que nunca. Miles de organizaciones en todo el mundo usan estos productos para una variedad infinita de funciones críticas para determinadas empresas.[5]

2.2.1 Elasticsearch

Elasticsearch es un motor de búsqueda y análisis de texto completo altamente escalable y de código abierto. Permite almacenar, buscar y analizar grandes volúmenes de datos de forma rápida y casi en tiempo real. Lo que esto significa es que hay una ligera latencia (normalmente un segundo) desde el momento en que indexa un documento(dato) hasta el momento en que se convierte en un dato a buscar.

Aquí hay algunos ejemplos de casos de uso para los que Elasticsearch podría usarse:

- Dirige una tienda web en línea donde permite a sus clientes buscar los productos que vende. En este caso, se puede usar Elasticsearch para almacenar todos los catálogos de productos e inventario y proporcionarles búsquedas y sugerencias de autocompletamiento a los clientes.
- Desea recopilar datos de registro o transacción para luego analizar y extraer estos datos y buscar tendencias, estadísticas, resúmenes o anomalías. En este caso, puede usar Logstash (parte del Elastic stack) para recopilar, agregar y analizar sus datos, y luego debe alimentar estos datos en Elasticsearch. Una vez estando los datos en este último, se podrá ejecutar búsquedas y agregaciones para extraer cualquier información que sea de su interés.[6]

Elasticsearch [7], es una base de datos NoSQL

[2] Conjunto de reglas oficiales elaboradas y actualizadas por Vulnerability Research Team (Equipo de Investigación de Vulnerabilidades)

[3] Command & Control es una forma de referirse a los servidores con la función de dar instrucciones al malware.

orientada a documentos en formato JSON y basada en Apache Lucene. Es una herramienta ampliamente utilizada en motores de búsquedas de texto en documentos de datos, proporcionando funcionalidades con muy baja latencia, dado que los datos están indexados. Elasticsearch permite configurar un clúster con distintos nodos a través del cual se distribuirán los datos, para después realizar búsquedas sobre ellos. En todo clúster debe haber un nodo de datos y un nodo maestro. El primero, se encargará de almacenar los datos y ejecutar las consultas y el nodo maestro será el encargado de dirigir el clúster, ordenando la ejecución de consultas, recuperando índices corruptos, etc.

Los datos se introducen en Elasticsearch en índices y las búsquedas se restringen a un único índice, es decir, no se pueden realizar búsquedas en los resultados que provengan de dos índices distintos. Esto da muchas veces lugar a redundancia de datos ya que cada índice se genera exclusivamente a partir de un documento. Para evitarlo, se pueden definir alias, bajo los cuales se agrupan varios índices, de tal forma que, realizando una búsqueda sobre un alias, se pueden realizar búsquedas sobre varios índices a la vez.

El almacenamiento de los datos en los nodos es gestionado directamente por el clúster, por medio de dos parámetros configurables por el usuario. El primero se denomina Shard y hace referencia al número de partes en que se dividirá un conjunto de datos para repartirlo por los nodos de datos del clúster. El segundo parámetro se denomina Factor de Replicación, con el que se especifica cuantas réplicas en otros nodos se hará de cada uno de los shards, para no perder datos en caso de fallo en alguno de los nodos de datos. Por ejemplo, en la siguiente figura se muestra el esquema de un clúster Elasticsearch con tres nodos de datos a través de los cuales se almacena un índice, el cual se ha dividido en 3 shards. Cada uno de estos shards se ha distribuido por los 3 nodos, y, por cada shard principal se ha generado una réplica. Las réplicas de estos shards también se han distribuido, pero por nodos distintos al nodo con el shard principal.

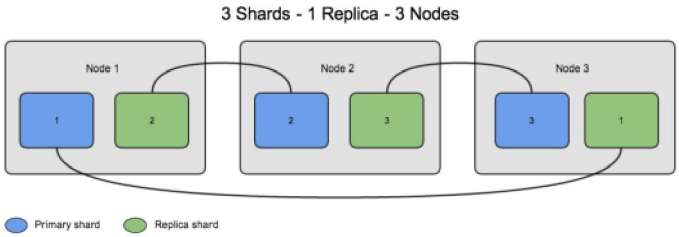

Figura 1 Almacenamiento de datos en shards y réplicas en Elasticsearch [7]

Elasticsearch se gestiona mediante una API REST, así que todas las peticiones se realizarán por medio de métodos HTTP. Estas peticiones tendrán por objetivo añadir índices, añadir datos a un índice, borrar un índice (nunca elementos individuales de un índice), consultar datos de un índice, etc. Además, los índices almacenados se podrán consultar por medio de un navegador web accediendo al servidor Elasticsearch y navegando por la jerarquía de índices. Elasticsearch tiene la posibilidad de añadir plugins que proporcionan una interfaz gráfica web con la que realizar las peticiones sobre Elasticsearch, navegar sobre los índices añadidos o consultar cada una de las entradas de los índices, por ejemplo, Plugin Head, una interfaz muy simple que nos permite consultar el estado del clúster, los índices creados, los datos insertados en cada índice o realizar peticiones. En la figura 2 se muestra la página principal de este plugin.[7]

En ella aparece una entrada por cada nodo que compone el clúster Elasticsearch. En la primera entrada, cada columna representa un índice cargado en Elasticsearch. En cada uno de los cruces nodo – índice se indica que shard de ese índice se almacenan en ese nodo.

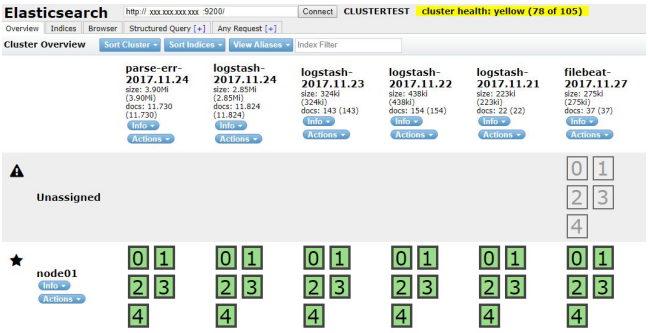

Figura 2 Página principal de Plugin Head.

2.2.2 *Logstash*

Logstash es una aplicación java de código abierto con el objetivo de transportar, recolectar, filtrar e indexar logs. La arquitectura de Logstash está compuesta por tres componentes principales en forma de plugins: Entrada, Filtro y Salida.

Los plugins de Entrada habilitan el soporte de Logstash para diversas fuentes generadoras de logs. Los plugins de Filtro permiten el procesamiento, incluidos filtrado y normalización, de los logs recolectados en las fuentes. Por último, los de Salida, posibilitan el envío de los logs recolectados y procesados a su

destino final.[8]

Si bien Logstash originalmente impulsó la innovación en la recopilación de registros, sus capacidades se extienden mucho más allá de ese caso de uso. Cualquier tipo de evento puede ser enriquecido y transformado con una amplia gama de entradas, filtros y plugins de salida, con muchos códecs nativos simplificando aún más el proceso de la ingesta.

Esto permite modificar los registros para almacenar toda la información necesaria, en el formato que más nos interese y de la forma más óptima.

La aplicación se encuentra basada en jRuby y requiere de una "Java virtual Machine" para funcionar. Gracias a esto la herramienta es multiplataforma, pudiendo ser ejecutada en cualquier sistema operativo moderno como Linux, Mac OS X o Windows.

Otra ventaja de Logstash respecto a sistemas basados en syslog es que ha sido creada por el mismo desarrollador que la base de datos. Esto asegura que no habrá incompatibilidad entre las diferentes piezas de la implementación.[4]

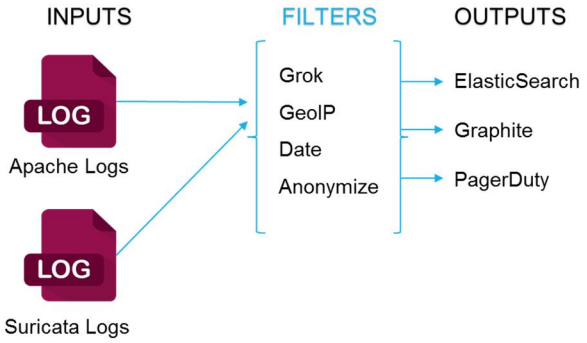

Figura 3 Arquitectura de Logstash.

2.2.3 Kibana

Kibana es una herramienta de visualización y exploración de datos. Entre las principales características que presenta se encuentran: integración completa con Elasticsearch, vistas personalizadas, análisis incorporado y soporte multiorigen.[8]

Kibana se puede usar para buscar, ver e interactuar con los datos almacenados en los índices Elasticsearch, de tal forma que se puede realizar fácilmente análisis avanzados de datos y visualizar estos datos en gran variedad de gráficos, tablas y mapas, todo ello por medio de una interfaz web.[7]

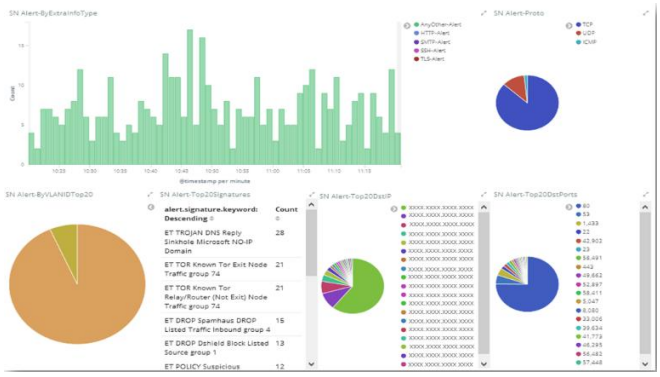

Figura 4 Visualización con Kibana

2.3 Firewall

Este dispositivo, que es la primera capa de seguridad, nos permite filtrar las conexiones entrantes a nuestra plataforma de modo que seamos capaces de definir políticas con respecto a qué tipo de protocolos pueden utilizarse para consultar nuestras aplicaciones publicadas.

Habitualmente en una plataforma dedicada a las publicaciones Web, estarán activadas las comunicaciones contra el puerto en el que esté publicado el servicio HTTP y, si además tenemos conexiones seguras, el puerto HTTPS.

De esta manera, somos capaces de restringir el acceso a nuestros equipos protegidos para que únicamente se redireccionen peticiones hacia nuestros equipos frontales cuando dichas comunicaciones sean, supuestamente, legítimas.

No obstante, estas comunicaciones, aunque sean conexiones lícitas para la plataforma, pueden contener códigos maliciosos que podrían suponer un riesgo para la plataforma si alguna de nuestras publicaciones sufre algún tipo de vulnerabilidad conocida.

El firewall realmente nos define un filtro que únicamente dejará pasar las comunicaciones que cumplan ciertos criterios (por ejemplo, comunicaciones contra una dirección IP en concreto que vengan por los puertos permitidos), es decir define una pequeña ventana entre todos los servicios disponibles en Internet.[9]

Entre las funciones más habituales de los firewalls tenemos[10]:

- Autorización o denegación de tráficos.
- Registro de las comunicaciones entre redes.
- Encaminamiento ("routing") de paquetes entre redes.
- Segmentación y securización de las grandes redes.

Esta labor se realiza a través de un motor de inferencia basado en reglas. Estas reglas son configuradas

por los administradores con el fin de autorizar o denegar comunicaciones.

.

2.4 Filtrado antispam

El filtrado antispam permite evitar que la empresa se vea inundada por infinidad de fastidiosos mensajes de correo electrónico no deseados, que consumen tiempo y muchas veces resultan peligrosos.

El filtrado antispam es un componente imprescindible en todo kit de herramientas de seguridad de red. Evita que los mensajes de correo electrónico no deseados inunden las bandejas de entrada de los empleados. Además, las soluciones antispam protegen contra los virus más recientes, los ataques de phishing y otras amenazas que llegan por correo electrónico.

En condiciones ideales, conviene comprar un dispositivo antispam que:

- Detenga los mensajes de correo no deseados, los virus y otro tipo de software malicioso antes de que lleguen a los servidores de correo electrónico.
- Ofrezca una instalación sencilla, basada en un navegador web, para poder instalarlo con rapidez y facilidad, y comenzar a trabajar de inmediato.
- Brinde una defensa que se actualice de forma constante y automática, por lo que protege a la empresa contra amenazas emergentes de rápida propagación.
- Se adapta a las necesidades y al presupuesto de su empresa.[11]

2.5 Resultados obtenidos hasta el momento

Como parte de las tareas de supervisión de la seguridad informática durante la realización de eventos y visitas de primer nivel en el país, el COS estableció un grupo para la respuesta a incidentes de seguridad, dedicado al monitoreo del tráfico malicioso en los puntos de agregación de los servicios. Como resultado del mismo, se ha logrado tener una visibilidad de las amenazas, incidentes y hechos de fraude asociados a estos servicios.

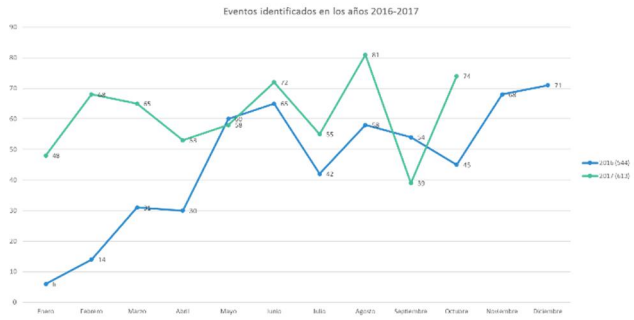

Figura 5 Gráfico de eventos en los años 2016 y 2017

2.6 Cleaning Center. Un nuevo servicio

Los resultados y experiencia adquirida en el proceso de conceptualización e implementación para el control de tráfico malicioso en los puntos de presencia de los servicios (PoP), ha arrojado la propuesta de ofrecer un nuevo servicio destinado a las empresas.

Este servicio, denominado Cleaning Center, tiene la funcionalidad de detectar y mitigar cualquier tipo de amenaza, programas maliciosos, entre otros, y dar respuesta ante este tráfico no deseado.

Cleaning Center proveerá a los clientes de un acceso a internet con una capa de seguridad adicional para protegerlos de un entorno de amenazas en constante evolución detrás del acceso. Con esta solución, todo el tráfico de internet del cliente, entrante y saliente se redirige a través de la red troncal MPLS a la plataforma Cleaning Center, donde se filtra y se bloquea cualquier malware y tráfico no deseado.

Figura 6 Proceso de Cleaning Center.

Cleaning Center se basa en el conjunto de herramientas anteriormente expuestas trabajando como un todo y perfectamente integradas, a fin de, ofrecer una mayor seguridad los usuarios que dispongan la contratación de dicho servicio. Entre sus principales características se encuentran las siguientes:

- **Firewall (IPS/IDS)**: Mecanismos basados en firmas que monitorean la red, detectan y detienen actividades maliciosas permitiendo o denegando el flujo de entradas y salidas, basándose en protocolo, puerto y dirección IP.
- **Filtrado web**: Mecanismos de clasificación de URL junto con un potente motor de reglas que permite la creación de políticas de acceso de internet. Limita la exposición a contenidos maliciosos e implanta políticas de uso de Internet corporativas.
- **Protección frente a amenazas**: prevención de intrusiones y bloqueo de software malicioso. Incluye funcionalidad de prevención de fuga de información basada en tipos de archivo y patrones.
- **Protección Antispam**: se basa en filtros de spam en lista negras de direcciones IP y URL, también sumas de verificación de correos.
- **Portal de servicio**: integrado a la plataforma de seguridad, con acceso a cuadros de mando en tiempo real, informe y visualizaciones de políticas de seguridad.

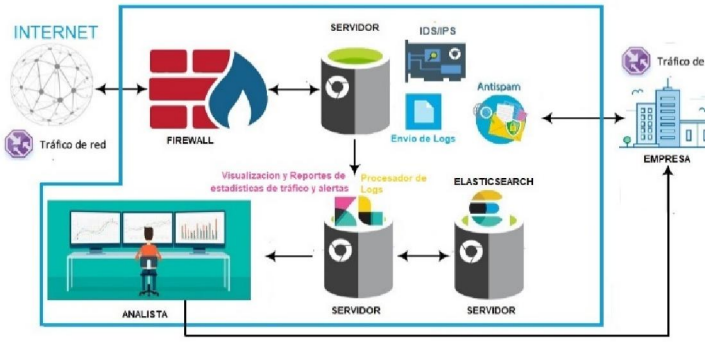

Figura 7 Estructura interna de Cleaning Center.

Cleaning Center es un servicio geográficamente redundante que elimina puntos únicos de falla y se ofrece únicamente desde la nube de seguridad de ETECSA. Con este modelo el cliente evita tener que adquirir y mantener soluciones de seguridad.

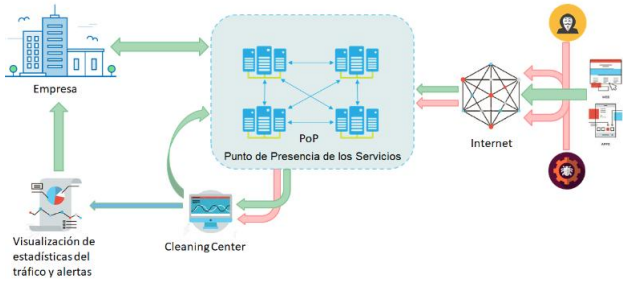

Figura 8 Funcionamiento del Cleaning Center

Además de las funcionalidades de protección, nuestros clientes cuentan con un portal de servicios donde pueden visualizar la actividad del servicio a través de cuadros de mando y reportes en tiempo real. Además de tener acceso para ver sus políticas de seguridad asociadas con los diferentes módulos del servicio.

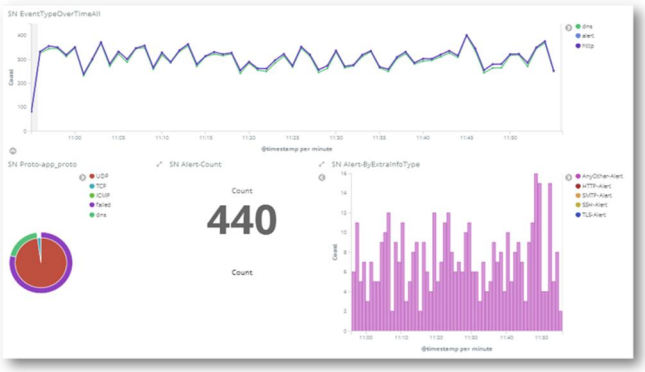

Figura 9 Cuadros de mandos Cleaning Center

2.7 ¿Porque usar Cleaning Center?

Cleaning Center, gracias a su poderosos IDS, detecta la existencia de computadoras vinculadas a redes botnet y programas malignos (incluidos ransomware y otros principalmente asociados a sistemas operativos de dispositivos móviles).

Tabla 1 Ejemplos de programas malignos detectados

MUESTRA DE PROGRAMAS MALIGNOS DETECTADOS	
Linux/XorDDoS	Win32/Sality
W32/Bayrob	Win32/Small
W32/Lethic	W32/Joiner.A
W32/Njw0rm	W32/Tempedreve
W32/Ramnit	Win32/Kido
W32/Rukap	Win32/Kido EJT
W32/Sality	Win32/Blaknight.A
Win/32 Dapato	Win32/Conficker
Win/32 Ramnit	Win32/Ursnif
Win32 / Floxif	Win32/Dreambot
Win32 / Glupteba	Win32/Qadars
Win32 / Injector.BRLE	Win32/Sohanad.AL
Win32 / InstallCore	TrojanDownloader W32/Carberp.A
Win32.Pushdo	Win32 / Recslurp.D
Backdoor.Win32.Rbot.adqd	Win32 / Xtrat.B
Backdoor.Win32.Rbot.bni	Win32/Blaknight.A
Botnet Lethic	Win32.Addrop
Win32/TrojanDownloader.Banload	Win32.Ammyy
Win32.Protux.B	Win32.Dapato

Como elemento común en las redes del país está la existencia de vulnerabilidades, la mayoría de estas conocidas desde hace varios años. Estas brechas de seguridad se encuentran en aplicaciones, sitios web, configuraciones de equipos entre otros elementos que interactúan en la red. El Cleaning Center permite identificar cuando una red está siendo objeto de escaneos en búsqueda de vulnerabilidades, previendo que sean explotadas posteriormente.

Los correos spam es otro de los comportamientos comunes en las redes empresariales cubanas ya sea como emisoras o receptoras del mismo, existiendo deficiencias en las configuraciones de los servidores de correo. El filtrado antispam realizado por Cleaning Center permite filtrar los mensajes entrantes ahorrando tiempo en no leer correos no deseados o spam y filtra toda la basura antes de que comience a consumir el ancho de banda ni utilizar el espacio en su servidor.

El siguiente gráfico muestra la cantidad de incidentes que han sido detectados y sus categorías estos datos sirven de ejemplo de lo que se podrá lograr con una implementación de Cleaning Center

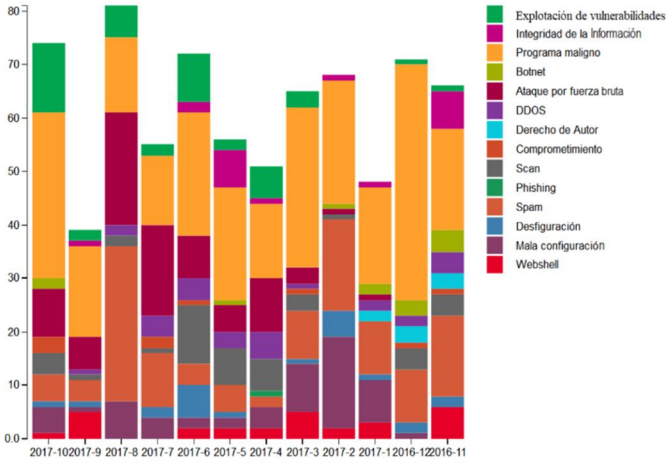

Figura 10 Ejemplo de incidentes detectados

3. CONCLUSIONES

El panorama de amenazas se encuentra en constante cambio, los atacantes emplean diversas técnicas avanzadas para sortear las herramientas de seguridad. Las amenazas basadas en malware, tales como ransomware, siguen siendo sumamente populares entre los atacantes. Además, las amenazas que no contienen malware, como phishing de credenciales, correos spam y vulneración de correo electrónico de empresas, afectan cada vez a más entidades. El uso del servicio de Cleaning Center permitirá disminuir, e incluso erradicar este tipo de amenazas mediante el filtrado del tráfico malicioso gracias a Suricata y a su función de IPS en el bloqueo de dicho tráfico.

Cleaning Center está diseñado como parte del servicio de acceso a Internet, de forma que la protección frente amenazas sea una característica esencial del servicio de acceso.

Con la contratación de dicho servicio, Cleaning Center proveerá a los usuarios de los siguientes beneficios:

- Proporcionar un plan completamente transparente de "pago por uso" sin costo adicional. Permite una drástica reducción de costo, el cliente no necesita invertir en hardware o software por lo tanto puede evitar los costos de mantenimiento, renovación y desarrollos tecnológicos.
- Garantizar el desarrollo continuo de actualizaciones para proteger la empresa en cuestión de las últimas amenazas, con esto poder garantizar la mejor tecnología de seguridad en un entorno de constante evolución de las amenazas de internet.
- Proporcionar protección completa de acceso a internet.
- Garantizar la disponibilidad de servicio cercana al 100% gracias a la arquitectura de alta disponibilidad y geográficamente redundante.
- Brindar al cliente un portal con informes y cuadros de mando en tiempo real.
- Tiene facilidad en la implementación, la gestión y el mantenimiento.
- Los administradores de redes de las empresas podrán completar con rapidez y facilidad las tareas de gestión, para que se centren en labores más estratégicas.
- El soporte técnico por parte de los especialistas de ETECSA les dará a las empresas que contraten el servicio la tranquilidad de saber que siempre recibirán ayuda especializada cuando la necesiten.
- Los administrativos podrán definir políticas de acceso a internet para su empresa, como sitios o contenidos no relacionados a su trabajo y que no desean que sean accedidos durante el horario laboral.

4. REFERENCIAS BIBLIOGRÁFICAS

1. Capraru Pons, C.A., *Detección de anomalías HTTP trazando la sesión web de un usuario*. 2016, Universidad Obrera de Catalunya.
2. *Suricata*. Available from: https://suricata-ids.org/.
3. *Caracteristicas de Suricata*. Available from: https://suricata-ids.org/features/.
4. Monte, A.A., *Diseño e implementación de*

infraestructura NIDS (Network Instrussion Detection System) para PIMES. 2017, Universidad Politécnica de Valencia.

5. *An Introduction to the ELK Stack*. Available from: https://www.elastic.co/webinars/introduction-elk-stack.
6. *Elasticsearch Getting Started*. Available from: https://www.elastic.co/guide/en/elasticsearch/reference/current/getting-started.html#getting-started.
7. Mínguez, A.R., *Mecanismos de análisis BigData para la caracterización de la actividad docente en un Campus Virtual Moodle*. 2016, UNIVERSIDAD DE VALLADOLID.
8. Ramírez, B.A.C., *Diseño e Implementación de una solución de gestion centralizada de logs de aplicaciones, sistemas y dispositivos basada en Logstash que permita la creación de cuadros de mando para explorar, analizar y monitorear eventos de seguridad.* 2015.
9. Molina, A.H., *Diseño, implementación y análisis de un sistema de detección y respuesta activa*. 2015, Universidad Autónoma de Madrid.
10. González, R.C.P., *Los sistemas de seguridad perimetral y principales vectores de ataque web*. 2016, Universidad Obrera de Catalunya.
11. Cisco, *Filtrado antispam: El fin del correo electrónico no deseado*

5. SÍNTESIS CURRICULARES DE LOS AUTORES

Ing. Javier Brooks Miranda. Nacido en La Habana el 17 de enero de 1988. Graduado de ingeniería en Telecomunicaciones y Electrónica en Instituto Politécnico Superior José A. Echeverría en el año 2012. Desde esa fecha ocupó el cargo de Especialista del Dpto. de Seguridad Informática en la División de Tecnologías de la Información en la Empresa de Telecomunicaciones de Cuba S.A. hasta el año 2014 donde comienza a desempeñarse como Especialista en el Centro de Operaciones de Seguridad de la Dirección de Operaciones de Seguridad de la misma entidad hasta la actualidad. Ha trabajado con el Sistema de gestión e información de eventos y seguridad, en temas relacionados con potes de miel, análisis y detección de intrusos y en la configuración y gestión de diferentes herramientas de seguridad. Ha participado en fórums de ciencia y técnica de su dirección y en los equipos de trabajo para los eventos de primer nivel.