UNIVERSIDAD NACIONAL AUTÓNOMA DE NICARAGUA

UNAN – León

Facultad de Ciencias y Tecnología

Departamento de Computación

Prevención de ataques de Ransomware conocidos en redes informáticas, utilizando la tecnología Check Point Sandblast en el perímetro y en usuarios finales comprendido en el periodo de septiembre del 2017 a abril del 2018

Tesis para optar al título de

Ingeniero en Telemática

Presentado por:

Br. Wing Lee Chow Zamora

Tutor:

Msc. Aldo René Martínez Delgadillo.

León, Abril 2018

Tabla de contenido

Índice de Figuras:

Resumen

En este trabajo monográfico se desarrolla una propuesta de seguridad para una empresa actual que implementa medidas de seguridad perimetral.

El proyecto se realizó para mitigar amenazas de Ransomware conocidos, ya que las soluciones tradicionales no tienen la capacidad de visibilizar malwares avanzados, que día a día aumentan en numerosas técnicas de ataques. Con la tecnología de Check Point se demostrará como resolver casos conocidos y avanzados con la herramienta que actualmente ofrece esta marca.

El trabajo está dirigido para las grandes y medianas empresas, y ayudarles en cómo prepararse ante cualquier incidente y mitigarlos en tiempo real.

La solución propuesta (Check Point Sandblast) fue implementada en un entorno virtual, ya que es más práctico para las demostraciones. También se realizó una topología previa en la que se agregó protecciones tradicionales que se encuentran en las empresas tales como Servidores y estaciones de trabajo.

Dentro de la topología se tiene un esquema de seguridad para ataques de Ransomware conocidos con una administración unificada.

CAPÍTULO 1 INTRODUCCIÓN

1.1 Antecedentes

Los ataques informáticos han estado evolucionando desde los primeros virus que aparecieron desde hace muchos años, hasta los malwares avanzado que atacan con diferentes vectores. Hoy en día existen múltiples problemas de cómo y cuándo mitigarlos en tiempo real. **Ataque de día cero (Zero Day Attack)** es un tipo de ataque contra equipos aprovechando una vulnerabilidad desconocida por los usuarios y los creadores de aplicaciones, para los cuales en ese momento no se tiene un parche, solución o actualización que corrigia dicha vulnerabilidad. Mientras la vulnerabilidad no es solucionada los equipos están totalmente desprotegidos a este tipo de ataques y a nuevos malwares. Cabe mencionar que el ataque Día Cero es en la actualidad el más peligroso y crítico que pueda haber.

Los equipos tradicionales no están preparados ante cualquier amenaza, y actualmente hay soluciones empresariales que se están usando en la Empresas que están expuestas ante cualquier malware tales como Ransomware que son las últimas generaciones de malware que constantemente evolucionan y son creados para atacar empresas como grandes y medianas Empresas de Telecomunicaciones, Bancos, etc.

Se tiene un esquema de tipos de malware que utilizan métodos de encriptación y que han evolucionado durante estos años:

- AIDS Trojan in 1989
- Donated Funds to AIDS Foundation
- Gpcode/Troj.RANSOM.A in 2006
  RSA Encryption via .EXE
- CryptoLocker, 2048 bit RSA key in 2013
- Gaming network delivery
  Payment via BitCoin
- CryptoWall in 2014
- Malvertising / Social Engineering
- $320M in BitCoin!
- Tesla Crypt 2015
  Utilized Angler Exploit Kit
  Some with embedded key
- KeRanger in March, 2016

1st Mac Crypto
- Wanna Cry May 12, 2017

Para la solución ante cualquier amenaza de malware avanzados se debe de tener productos de ciberseguridad dentro de la infraestructura de la empresa para así tener la visibilidad de los que está pasando y poder mitigar esos ataques en diferentes vectores. Los ataques informáticos están a la orden del día. Afortunadamente, existen soluciones disponibles que permiten proteger el perímetro con un sistema de detección de intrusos basados en reglas, que evita las conexiones no deseadas para ataques conocidos.

Hoy en día todavía no existe algún estudio monográfico de la herramienta de Sandblast, pero si casos exitosos con respecto a la experiencia de la solución tales como:

- Centroamérica y América del Sur:
    - Centroamérica: Banca y finanzas (como BANPRO), Instituciones del estado (Policía Nacional), Empresas industriales, Empresas de publicidad entre otros.
    - América del Sur: Colombia es uno de los países más afectados por Ransomware junto a Ecuador, los cuales han sido lo más atacados en el período 2014 – 2017. En estos países, los Bancos y las instituciones del estado trabajan día a día con la herramienta de prevención de amenazas avanzadas y desconocidas dirigidas al país.

1.2 Planteamiento del Problema

Debido a la alta tasa de ataques informáticos Check Point creó una solución de prevención en tiempo real llamado Sandblast para ataques avanzados basada en los **Sandboxing** (Mecanismo de detección y prevención de malwares) tradicionales, pensadas para las empresas que cuentan con soluciones de seguridad perimetral con poca capacidad de enfrentar a malware con nuevas técnicas. Eso hace más vulnerable a robos de datos y encriptamiento de máquinas que hoy en día los Firewall tradicionales están expuesto a dicho ataque.

Los usuarios tales como gerentes, analistas, etc buscan una solución para la protección de datos personales y de trabajo que le permita estar seguro ante cualquier ataque de Malware Avanzado:

1. **Troyano para mantener una red BotNet.**

Las máquinas contaminadas se vuelven máquinas zombies y son controlados desde Internet a través de un Command & Control. En este caso el objetivo del atacante es tener presencia en la red y hacer pivote de la máquina controlada hacia el centro de datos para robar los datos (Exfiltrar los datos).

2. **Troyano Bancario.**

Es un troyano especial que detecta cuando el usuario está haciendo transacciones con la aplicación de banca en línea.

3. **Ataque de Ransomware (Secuestro de información)**

El ataque de Ransomware se hace aprovechando vulnerabilidades en:

a. Browser y en los componentes de los mismos (plugins de Java, Plugins de Flash, Plugin de Adobe PDF reader).

b. PDF Reader como Adobe (links embebidos en documentos PDF)

c. Documentos de Office que tiene código de ejecuciones embebidas.

Pregunta General:

¿Es CheckPoint la tecnología adecuada y completa para proteger la red informática de una Empresa, de los ataques de Ransomware?

Preguntas específicas:

¿Cuáles son las principales afectaciones que se dan con un ataque de Ransomware Cerber, Goldeneye y Criptolocker en los sistemas operativos, archivos y aplicaciones de una red informática?

¿Cuáles son las estrategias y planes de seguridad informática que debe tener una Empresa, para prevenir ataques de Ransomware?

¿Qué ventajas aporta en términos de precio y rendimiento, frente a otras tecnologías, la solución de CheckPoint SandBlast, para afrontar los ataques de Ransomware?

1.3 Justificación

Con la presente investigación se obtendrá la capacidad de detectar y prevenir con la tecnología Check Point, los malwares Cerber, Goldeneye y Criptolocker que tienen mecanismos de evasión avanzadas dirigidas hacia soluciones tradicionales.

Con esta tecnología se brindará conocimientos acerca de cómo Check Point ha estado ayudando a las compañías a mejorar sus mecanismos de ciberseguridad.

Originalidad

Este trabajo será original, ya que se hablará de cómo Check Point ha incorporado dentro de la solución de Sandblast Network las siguientes capas de seguridad:

- Antivirus
- Extracción y reconstrucción de archivos
- Detección a nivel de CPU
- Emulación de archivos dinámicamente (**Sandboxing** Tradicionales)

Check Point es el único producto que ofrece una detección y prevención completa para ataques de Ransomware.

Alcance

Una vez realizadas todas las configuraciones recomendadas en la plataforma Check Point brindará al administrador las siguientes análisis antes (alertas), durante (Prevención) y después del ataque (Análisis Forénsico) :

- Visibilidad de estaciones de trabajos infectados.
- Análisis de Logs durante la prevención del ataque.
- Reportes forénsicos de los eventos en tiempo real del ataque.

Producto

El producto se presentará dentro de una topología virtualizada en la nube con seguridad perimetral, con redes internas y externas, junto a una zona desmilitarizada (DMZ) para la protección de las siguientes funcionalidades:

- Firewall
- NAT
- Identity Awareness (Identidad de Usuario)
- Antibot
- Antivirus
- Sandblast (Threat Emulation and Threat Extraction).

Impacto

Este documento permitirá a las Empresas que utilicen la tecnología Check Point, una mayor seguridad perimetral y de usuario final con una plataforma consolidada.

1.4 Objetivos

1.4.1 Objetivo general

Evaluar si la tecnología SandBlast de Checkpoint, es la opción más viable para proteger la red informática de una empresa de los ataques de Ransomware Cerber, Goldeneye y Criptolocker.

1.4.2 Objetivos específicos

- Demostrar los ataques de Ransomware Cerber, Goldeneye y Criptolocker en el perímetro y en usuarios finales de una red Informática, con y sin la tecnología CheckPoint Sandblast.

- Detallar las estrategias, políticas y planes de Seguridad Informática que ofrece Check Point para las Empresas.

.

- Mostrar las ventajas que aporta en términos de complejidad y rendimiento, frente a otras tecnologías, la solución de CheckPoint, SandBlast, para afrontar los ataques de Ransomware.

CAPÍTULO 2 MARCO TEÓRICO

2.1 Check Point Software Technologies

2.1.1 Historia

Establecido en 1993, por el CEO Gil Shwed, Check Point fue pionero el I.T. con FireWall-1 y su tecnología de inspección patentada Stateful, que sigue siendo la base para la mayoría de la tecnología de seguridad de red hoy en día.

Desde que comenzó la compañía, el enfoque puro de Check Point ha estado en I.T. seguridad. Adaptándose a las necesidades cambiantes de los clientes, la compañía ha desarrollado numerosas tecnologías para asegurar el uso de Internet por corporaciones y consumidores al realizar transacciones y comunicarse. En 2006, Check Point creó una arquitectura de seguridad unificada, utilizando una única consola de administración, Firewall de seguridad unificada y el primer y único agente para la seguridad de los puntos finales. A principios de 2009, Check Point introdujo una nueva innovación de seguridad con su arquitectura Software Blade: una arquitectura dinámica y revolucionaria que ofrece soluciones seguras, flexibles y sencillas que pueden personalizarse totalmente para satisfacer las necesidades de seguridad exactas de cualquier organización o entorno.

En abril de 2009, la Compañía completó la adquisición del negocio de dispositivos de seguridad de Nokia, después de más de una década de colaboración en la entrega de soluciones de seguridad empresarial líderes en la industria.

En noviembre de 2009, Check Point adquirió la base de datos de aplicaciones de FaceTime Communications, añadiendo controles de seguridad para más de 50.000 widgets Web 2.0 y más de 4.500 aplicaciones de Internet a nuestras pasarelas de seguridad.

Hoy en día, Check Point continúa desarrollando nuevas innovaciones basadas en la Arquitectura de Blade de Software, proporcionando a los clientes soluciones flexibles y sencillas que pueden ser completamente personalizadas para satisfacer las necesidades de seguridad exactas de cualquier organización. Check Point es el único proveedor que va más allá de la tecnología y define la seguridad como un proceso de negocio. Check Point 3D Security combina de manera única las políticas, las personas y la aplicación para una mayor protección de los activos de información y ayuda a las organizaciones a implementar un plan de seguridad que se alinea con las necesidades del negocio.

2.2 Check Point Zero Day Protection (Check Point Protección de día cero)

Los hackers modifican constantemente sus estrategias y técnicas para evadir la detección y alcanzar los recursos corporativos. La protección de cero días de Check Point proporciona un nivel de inspección más profundo para que pueda evitar más ataques de malware y de día cero, a la vez que garantiza la entrega rápida de contenido seguro a sus usuarios.

Obtener un paso por delante de lo desconocido

Las amenazas persistentes de día cero y avanzadas utilizan el elemento de sorpresa para eludir la seguridad tradicional, lo que hace que estas amenazas sean difíciles de proteger y muy populares entre los hackers. El **Sandboxing** es un mecanismo para ejecutar programas con seguridad y de manera separada. A menudo se utiliza para ejecutar código nuevo, o software de dudosa confiabilidad proveniente de terceros. El sandboxing tradicional fue diseñado para ayudar con este tipo de amenazas, pero los ciber delincuentes han desarrollado sus técnicas, creando malware evasivo que puede evitar la detección por muchas soluciones de Sandbox. Como resultado, muchas organizaciones se encuentran tomando medidas reactivas para contrarrestar la infección, en lugar de prevenirlo en primer lugar.

Para salir adelante, las empresas necesitan una estrategia de prevención multifacética que combine una protección proactiva que elimine las amenazas antes de que lleguen a los usuarios y una detección de vulnerabilidades de última generación para exponer incluso las amenazas más camufladas.

¿Qué es Sandblast?

Es una solución de prevención en tiempo real en contra de malware desconocido, de día cero, ataques dirigidos.

Figura 1 : Check Point Sandblast Components

2.3 Sandblast Network (Sandblast en Red)

2.3.1.1 Protección completa contra amenaza de día de cero

Check Point SandBlast Zero-Day Protection ofrece una protección completa contra los ataques más peligrosos de día cero y ataques dirigidos a la red, utilizando dos tecnologías principales: emulación de amenazas y extracción de amenazas.

La combinación de estas tecnologías de vanguardia hace que SandBlast sea el único capaz de identificar las amenazas de día cero más sofisticadas antes de que el malware tenga la oportunidad de desplegar e incluso intentar evadir la detección, garantizando al mismo tiempo la entrega rápida de contenido seguro a los usuarios.

2.3.1.2 Detección resistente a la evasión

A diferencia de otras soluciones, Check Point SandBlast Zero-Day Protection utiliza una tecnología única que realiza inspecciones a nivel de la CPU para detener los ataques antes de que tengan la oportunidad de lanzarse.

Hay miles de vulnerabilidades y millones de implementaciones de malware, pero hay muy pocos métodos que los ciberdelincuentes utilizan para explotar las vulnerabilidades. El motor de emulación de amenazas SandBlast de Check Point supervisa el flujo de instrucciones basado en CPU para intentos de evitar el sistema operativo y los controles de seguridad del hardware.

Detectando intentos de explotación durante la fase de preinfección, el Sandbox de Check Point SandBlast Threat Emulation detiene los ataques antes de que tengan la oportunidad de evadir la detección por el sandbox.

- **Captura más malware**

Check Point SandBlast Zero-Day Protection conduce una investigación más profunda con la emulación de amenazas de nivel OS interceptando y filtrando archivos entrantes e inspeccionando las URL vinculadas a archivos dentro de correos electrónicos ejecutándolos en un entorno virtual. El comportamiento del archivo se inspecciona simultáneamente en varios sistemas operativos y versiones. Los archivos que participan en actividades sospechosas comúnmente asociadas con malware, como la modificación del registro, las conexiones de red y la creación de nuevos archivos, se marcan y se analizan más a fondo. Los archivos maliciosos no pueden ingresar a su red.

- **El ecosistema de ThreatCloud**

Las amenazas recién descubiertas se envían a la base de datos de inteligencia de ThreatCloud. Cada nueva firma de amenaza descubierta se distribuye a través del ecosistema de ThreatCloud para proteger otras puertas de enlace conectadas a Check Point. Esto permite a las pasarelas conectadas bloquear la nueva amenaza antes de que tenga la oportunidad de extenderse. La colaboración constante hace que ThreatCloud sea la red de inteligencia de amenazas más avanzada y actualizada.

- **Prevención proactiva con pronta entrega de contenido seguro**

Cuando se trata de protección contra amenazas, no tiene por qué ser un intercambio entre velocidad, cobertura y precisión. A diferencia de otras soluciones, Check Point SandBlast Zero-Day Protection se puede implementar en detectar y prevenir el modo, al tiempo que mantiene un flujo de negocio ininterrumpido.

Nuestro componente de Extracción de Amenazas en Check Point SandBlast elimina las amenazas al eliminar contenido riesgoso, como macros o enlaces incrustados, y luego reconstruye el documento utilizando sólo elementos seguros conocidos.

A diferencia de las tecnologías de detección que requieren tiempo para buscar e identificar amenazas antes de bloquearlas, Threat Extraction elimina de forma preventiva el riesgo, garantizando la entrega rápida de documentos seguros.

- **Protege los tipos de archivo más comunes**

Check Point SandBlast Zero-Day Protection asegura una amplia gama de los tipos de documentos más comunes utilizados en las organizaciones de hoy, desde Microsoft Office Word, Excel, Power Point y PDFs de Adobe para archivar archivos.

- **Flexible y fácil de desplegar**

Check Point SandBlast Threat Emulation admite múltiples opciones de implementación, proporcionando una solución rentable para prácticamente cualquier organización de tamaño. Los archivos se pueden enviar desde pasarelas existentes al servicio basado en la nube de SandBlast oa un dispositivo local disponible con una gama de capacidades de rendimiento.

Instalado como una hoja de software adicional en la pasarela, Check Point SandBlast Threat Extraction se puede aplicar a toda la organización o implementarse solo para individuos, dominios o departamentos específicos. Los administradores pueden configurar usuarios y grupos incluidos según sus necesidades, facilitando fácilmente la implementación gradual en la organización.

- **Solución completa e integrada**

Check Point SandBlast Zero-Day Protection está totalmente integrado con Check Point Security Management, permitiendo la creación de políticas y perfiles de seguridad y la configuración desde una plataforma unificada. Check Point SmartEvent proporciona visibilidad e informes en el horizonte de amenazas de su organización, permitiendo una rápida investigación y resolución de eventos de seguridad.

2.4 Sandblast Agent (Sandblast en Agentes)

- **Evita el malware de día cero**

Check Point SandBlast Agent extiende las protecciones probadas de SandBlast Zero-Day Protection a dispositivos de punto final y navegadores web. Threat Extraction reconstruye los archivos descargados en segundos, eliminando posibles amenazas y entregando una versión segura a los usuarios. Al mismo tiempo, Emulación de amenazas detecta comportamientos maliciosos e impide la infección de nuevos programas maliciosos y ataques dirigidos, inspeccionando rápidamente los archivos en un entorno de seguridad virtual.

- **Prevenir los ataques de Ransomware**

La capacidad de Ransomware de evitar algunas de las protecciones de malware más avanzadas ha afectado a las empresas de todo el mundo. Check Point Anti-Ransomware mantiene las empresas un paso por delante de los ataques detectando, bloqueando y eliminando automáticamente las infecciones de ransomware más sofisticadas y restaurando los datos cifrados como parte de su capacidad de remediación automatizada.

- **Bloquea ataques de phising de día cero**

La capacidad de Phishing cero en SandBlast Agent utiliza análisis dinámico y heurísticas avanzadas para identificar y prevenir el acceso a sitios de phishing nuevos y desconocidos dirigidos a las credenciales de usuario a través de navegadores web en tiempo real. Además, esta capacidad evita el robo de credenciales corporativas de posibles infracciones de contraseñas en sitios de terceros al alertar a los usuarios cuando violan las políticas de reutilización de contraseñas corporativas.

- **Identifica y contiene infecciones**

Con una versión local de la protección de seguridad Anti-Bot, actualizada continuamente con los últimos datos de Threat Intelligence a través de ThreatCloud, SandBlast Agent identifica y bloquea las comunicaciones bot con los servidores de comando y control para contener y poner en cuarentena a los hosts infectados.

- **Cobertura integral de los vectores de amenazas**

El Agente SandBlast protege los dispositivos de punto final de amenazas enviadas a través de:

Descargas web
Contenido copiado de dispositivos de almacenamiento extraíbles
Enlaces o archivos adjuntos en mensajes de correo electrónico
Movimiento lateral de datos y malware entre sistemas en un segmento de red infecciones transmitidas a través de contenido cifrado.

- **Visibilidad completa de los eventos de seguridad**

La capacidad forense del agente SandBlast proporciona una visibilidad completa mediante el seguimiento y registro de todos los eventos de punto final, incluidos los archivos afectados, los procesos iniciados, los cambios en el registro del sistema y la actividad de la red. SandBlast Agent es capaz de rastrear y reportar los pasos tomados por el malware, incluyendo amenazas de día cero. El monitoreo continuo por SandBlast Agent asegura que los datos estén disponibles después de un ataque completo, incluso aquellos basados en técnicas de malware que eliminan archivos y otros indicadores de compromiso dejados en el sistema.

- **Informes de incidentes detallados**

La capacidad forense de SandBlast Agent le permite ver informes de eventos, desencadenados desde la puerta de enlace o el punto final en sí, desde una ubicación central mediante SmartEvent. Los administradores de seguridad también pueden generar informes para eventos maliciosos conocidos, proporcionando un análisis detallado de la cadena de eliminación de virus. Estos informes proporcionan un análisis de incidentes accionables, acelerando el proceso de comprensión del ciclo completo de ataque, daños y vectores de ataque.

- **Integración con terceros**

La capacidad forense de SandBlast Agent le permite ver informes de eventos, desencadenados desde la puerta de enlace o el punto final en sí, desde una ubicación central mediante SmartEvent. Los administradores de seguridad también pueden generar informes para eventos maliciosos conocidos, proporcionando un análisis detallado de la cadena de eliminación de virus. Estos informes proporcionan un análisis de incidentes accionables, acelerando el proceso de comprensión del ciclo completo de ataque, daños y vectores de ataque.

- **Análisis de incidentes realizables**

El proceso de análisis forense se inicia automáticamente cuando se produce un evento de malware. Usando una combinación de algoritmos avanzados y un análisis profundo de los datos forenses brutos, construye un resumen de incidentes completo. El resumen proporciona información clave de ataque accionable, que incluye:

Eventos malintencionados - ¿Qué evidencia de comportamiento sospechoso fue detectada durante el ciclo de vida del ataque?

Punto de entrada –

- ¿Cómo entró el ataque en la red?
- ¿Cuáles fueron los principales elementos utilizados en el ataque?
- ¿Cómo se inició el ataque?
- Alcance de daños –

- ¿Cuál es el daño?
- ¿Qué comportamiento malicioso y sospechoso ha ocurrido dentro del sistema?
- ¿Qué datos han sido robados?
- Hospitales infectados –
- ¿Quién más o qué más se ve afectado?

Este completo diagnóstico de ataques y visibilidad soporta los esfuerzos de remediación. Los administradores de sistemas y los equipos de respuesta a incidentes pueden tripar y resolver ataques de forma rápida y eficiente, haciendo que su organización vuelva a operar como de costumbre más rápido.

CAPÍTULO 3 DISEÑO METODOLÓGICO

En esta sección se enumeran los diferentes materiales empleados en este trabajo y se describen las etapas a través de las cuales se abordó nuestra investigación.

3.1 Materiales utilizados:

3.1.1 Hardware

Los materiales hardware empleados en nuestro trabajo fueron:

Materiales Hardware Físico y Virtual

Material	Descripción	Costo aproximado
Laptop	Cuatro procesadores AMD A4-5000 APU with Radeon HD Graphics 1.5 GHZ. Memoria RAM DDR3 de 4GB. Esta laptop actuará como el cliente de administración de políticas	$300
Check Point Security Gateway (Ubicado en la nube)	Procesador: 4 cores Memoria: 4 GB Disco Duro: 80 GB Interfaces: 3 (Interna, DMZ y Externa)	Serial de prueba generado como Partner de Check Point (Wing).
Check Point Security Management (Ubicado en la nube)	Procesador: 4 cores Memoria: 4 GB Disco Duro: 100 GB Interfaces: 1 (DMZ)	Serial de prueba generado como Partner de Check Point (Wing).
Windows Server 2008 R2 (Centralizado en la nube)	Procesador: 4 cores Memoria: 2 GB Disco Duro: 40 GB Interfaces: 1 (DMZ)	Serial de prueba

3.1.2 Software

Materiales Software

Software	Descripción
CloudShare	Entorno virtual de trabajo para la creación y segmentación de la topología contralada.
Check Point R77.30 Gateway y Management	Es el sistema operativo oficial de Check Point llamado GAIA, con software blades unificado de ciberseguridad.
Microsoft Windows Server 2008 R2 y 7	Sistema operativo de Microsoft, que tiene muchas utilidades de servicios tanto para servidores y PC.
Kali Linux 2018.1	Sistemas operativos usados para cualquier ataque dirigido mediante herramientas basadas en Linux.

3.2 Etapas del proyecto

Para abordar y cumplir todos nuestros objetivos, se dividió el trabajo en las siguientes etapas:

3.2.1 Etapa I: de exploración

En esta etapa se recopiló información acerca del tema, haciendo búsquedas en libros, sitios web, etc.

3.2.2 Etapa II: Creación e instalación de máquinas virtuales Check Point, Windows Server y 7, y Kali Linux y demostración del ataque de Ransomware conocido.

En esta etapa se crearon máquinas virtuales para la topología de la red controlada. Para esto se realizaron una serie de sub-etapas que se describen a continuación:

3.2.2.1 Máquina virtual Firewall Gateway y Management (Check Point Gateway e Management)

En esta prueba se crearon dos máquinas virtuales Check Point tanto para Gateway y Management comuniquen entre sí a través de la micro-segmentación del CloudShare.

3.2.2.2 Máquina virtual del atacante (Kali Linux)

Se estará utilizando una maquina atacante en este caso un Kali Linux para dichos ataques dirigidos hacia las maquinas PC internas sin y con Agentes de Sandblast. Los Ransomware ya están creados en las máquinas víctimas para la demostración de prevención del producto.

3.2.2.3 Máquina virtual del Windows Server 2008 R2 y las dos máquinas cliente en Windows 7.

Se crearon máquinas virtuales uno para el servidor de Directorio activos en la red DMZ y dos máquinas que van a interactuar como clientes en la red interna.

3.2.3 Etapa III: Configuración recomendada del Check Point Sandblast Network y Sandblast Agent.

En esta etapa se configuró el Check Point Gateway y Management de manera recomendada para el despliegue y análisis de Sandblast Network y Sandblast Agent, tomando como referencia las siguientes configuraciones:

- Se configuraron las interfaces de red y rutas de las redes que estarán detrás del Check Point como la red externa, DMZ e interna en el Gateway.
- Se generó una licencia válida para el Gateway de 30 días.
- Se configuró también el Security Management para el manejo de políticas hacia el Gateway, donde se activó los blades de Firewall, IPS, Antivirus, Antibot, Threat Emulation y Threat Extraction. Además, se configuró el SmartEvent (Análisis Forense y de Eventos) y el Endpoint Security Management.
- Se instaló hotfixes (Parches) en el Security Management para el correcto funcionamiento del Endpoint Security Server.
- Se configuró las políticas en el Endpoint Security para el despliegue del Sandblast Agent en la máquina víctima.

3.2.4 Etapa IV: Realización de pruebas de conectividad, funcionamiento y mecanismos de prevención de la herramienta.

Se hizo pruebas de conectividad de las redes de DMZ, Externa e interna, se procedió a validar pruebas de filtrado de Firewall, IPS, Application and URL Filtering, Antivirus, Antibot, Threat Emulation and Threat Extraction mediante el SmartLog y SmartEvent, cuyos resultados fueron exitosos y se pudo observar lo siguiente:

3.2.4.1 Análisis de Logs de prevención ante ataques conocidos y desconocidos hacia las máquinas víctimas vía MTA Sandblast Network.

Se determinó el origen y destino del ataque en tiempo real y se obtuvo un análisis forense de cómo es la naturaleza del Malware (Ransomware). Se utilizó un sistema de Sandboxing de detección a nivel de CPU, alimentada desde el ThreatCloud de Check Point.

3.2.4.2 Análisis de ataques hacia una máquina, mediante el SmartEvent del Sandblast Agent.

Se evaluó el análisis de archivos infectados (.doc) con la utilidad del Anti-Ransomware perteneciente del Sandblast Agent. También se bajaron, vía HTTP, archivos de tipo .doc maliciosos para el análisis y se hizo el bloqueo de ataques de comando y control procedente de la máquina víctima.

3.2.5 Etapa V: Redacción del informe final

Redacción y organización del documento final, el cual contiene la explicación de cada una de las etapas de este proyecto y solución de cada uno de los objetivos planteados.

CAPÍTULO 4 DESARROLLO

4.1 Configuración de red, póliticas de Firewall, Application and URL Filtering, IPS, Antivirus, Antibot, Threat Emulation y Threat Extraction.

Con Check Point se configuraron los siguientes blades, quedando de esta manera:

4.1.1 Interfaces de red Check Point Gateway:

En este primer escenario se logró configurar las siguientes interfaces, de acuerdo a la topología mostrada a continuación, y se realizó lo siguiente:

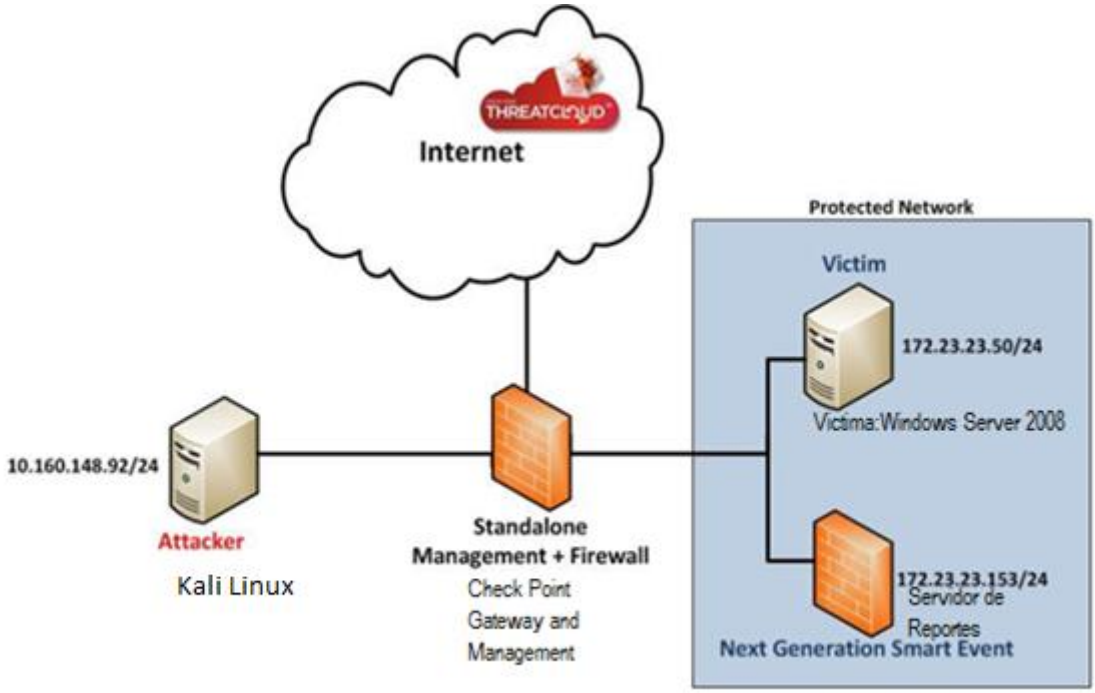


Figura 2: Topología Check Point Sandblast Network para la demo propuesta.

- Creación de interfaces de red GAIA:

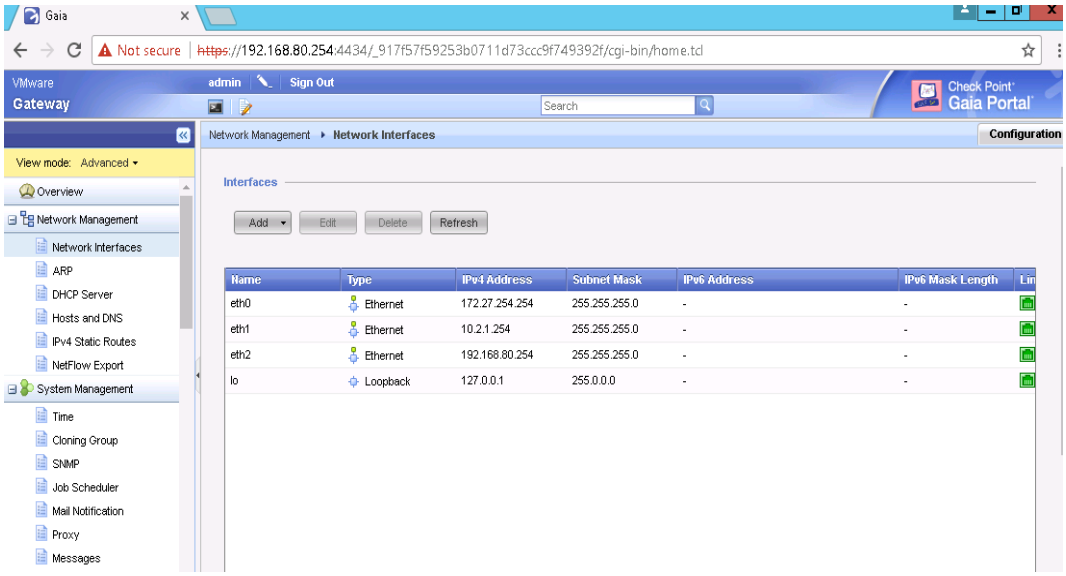


Figura 3: Portal de Check Point GAIA

En la actual topología se obtiene lo siguiente:

- Red externa: Interfaz donde pasará toda la navegación y donde estará el atacante.
- Red Interna: Interfaz donde estarán los usuarios finales.
- Red DMZ: Interfaz donde estará los servidores.

4.1.2 Creaciones de reglas de Firewall en Check Point.

Se crearon las siguientes reglas:

- Acceso hacia el Management.
- Acceso hacia la DMZ.
- Acceso desde la DMZ hacia la red interna.
- Bloqueo de administración del Management (Stealth Rule)
- Acceso hacia cualquier lugar mediante políticas basadas en usuarios.
- Acceso desde la red interna hacia la red externa y DMZ.

No.	Hits	Name	Source	Destination	VPN	Service	Action	Track
1	29	Management Access from Outside	Net-172.27.254	Gateway	Any Traffic	Any	accept	Log
2	14	Allow full access to DMZ	Net-10.2.1.0 Net-172.27.254	Net-192.168.80	Any Traffic	Any	accept	Log
3	162	Allow full access from DMZ	Net-10.2.1.0 Net-172.27.254 Net-192.168.80	Net-10.2.1.0 Net-172.27.254	Any Traffic	Any	accept	Log
4	75	Drop NBT do not log	Any	Any	Any Traffic	NBT	drop	None
5	8	Stealth Rule	Any	Gateway	Any Traffic	Any	drop	Log
6	0	Allow authenticated users	Identity-Awarei	Any	Any Traffic	Any	accept	Log
7	0	Allow internal network out	Net-10.2.1.0	Net-192.168.80 Net-172.27.254	Any Traffic	Any	accept	Log
8	0		Gateway Manager Host_192.168.8	Any	Any Traffic	dns ntp	accept	None
9	380	Drop everything else	Any	Any	Any Traffic	Any	drop	Log

Figura 4: Creación de reglas en el Firewall Blades

4.1.3 Ataque de Comando y Control con reglas de simple Firewall, análisis del ataque y activación del IPS, Antivirus, Antibot y Threat Emulation.

Se hizo un ataque de comando y control hacia la maquina víctima y se hicieron pruebas del ataque exitoso:

- Se lanza el ataque mediante la herramienta de Ghost RAT, Troyano instalada en la maquina víctima desde la red externa hacia la red interna:

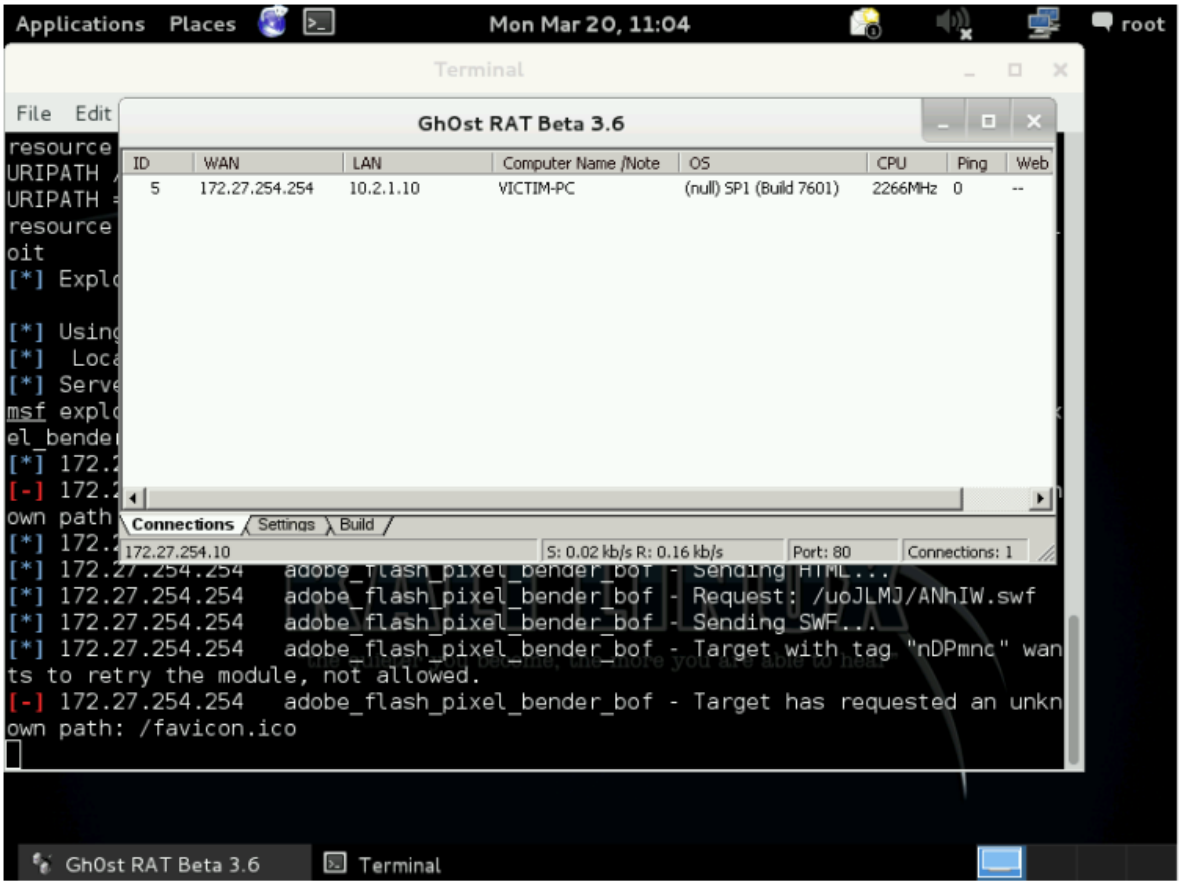


Figura 5: Ataque de comando y control desde la red externa

- La máquina víctima se ha descargado un programa vía HTTP del servidor Apache (Kali Linux), el cual ha sido instalado en el sistema operativo de la maquina víctima haciendo cambios en los registros de Windows, donde se ejecuta el proceso metasploit , donde se procedió a abrir las carpetas o rutas de los directorios de la máquina víctima de manera remota. El cual se verificó en los Logs del Security Management, donde no se encontró absolutamente nada (a como un simple Firewall tradicional podría trabajar).

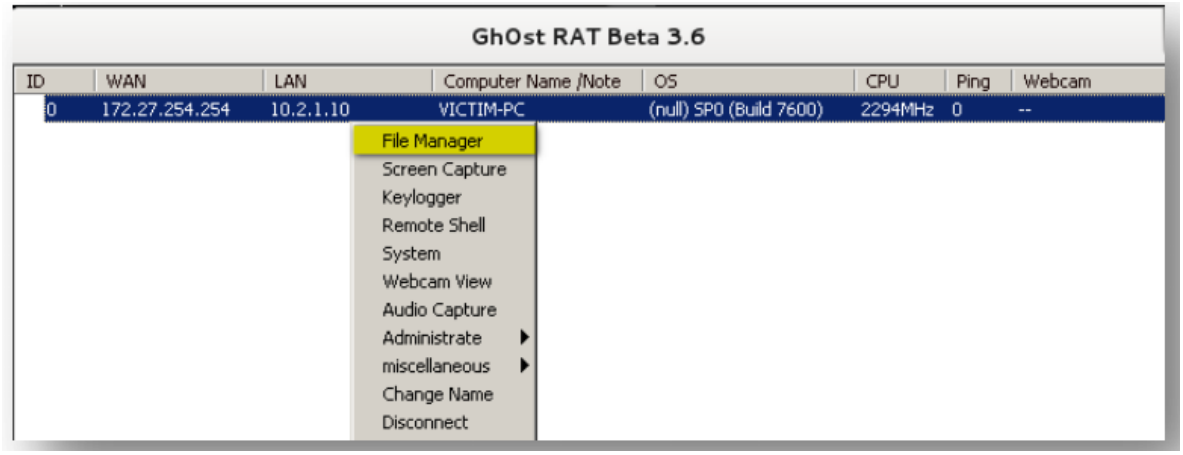


Figura 6: Ingreso a las carpetas de la víctima

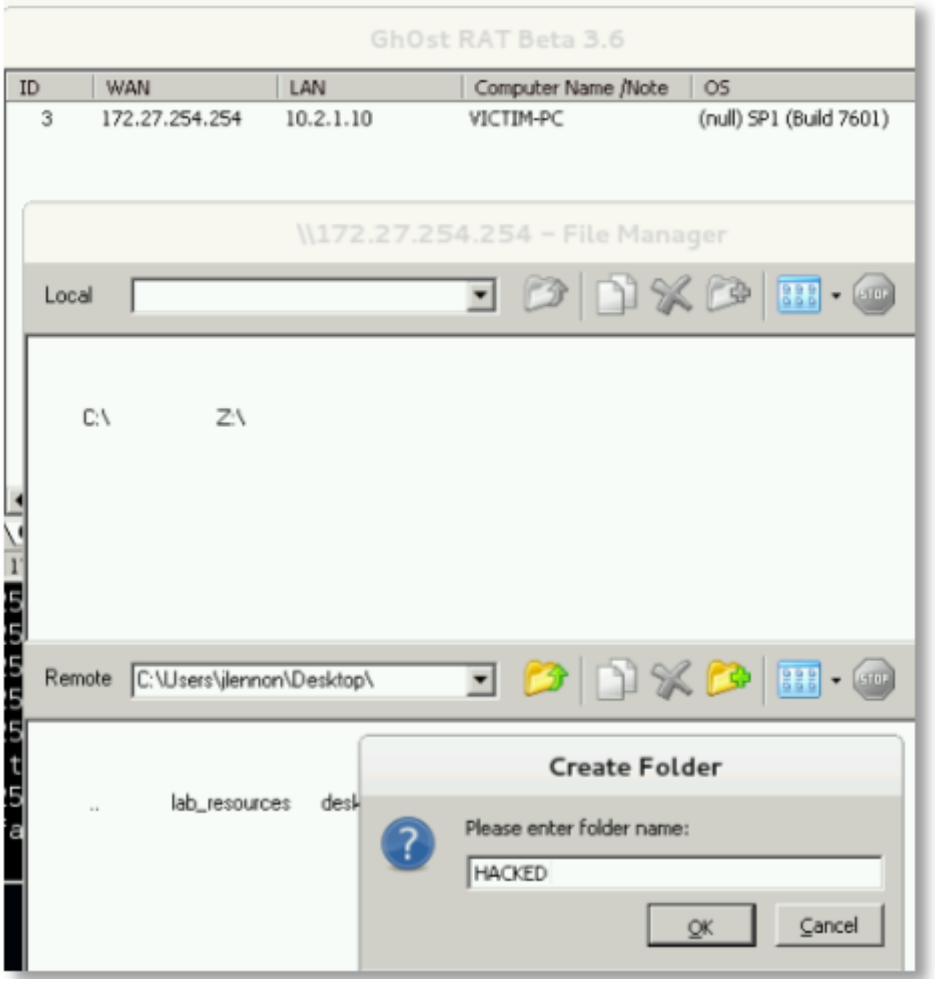


Figura 7: Creación de carpeta dentro de la máquina víctima

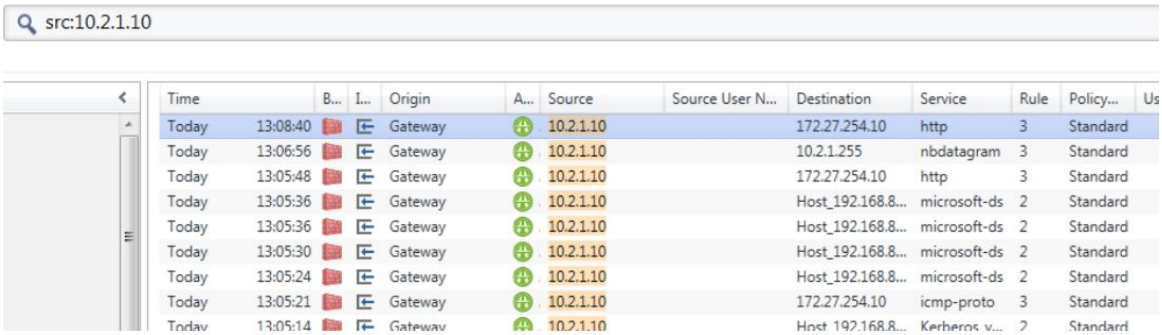


Figura 8: Verificación de Logs de Simple Firewall

A continuación, se activarán y se configurarán blades recomendados para la prevención de ataques conocidos y Ransomware en el perímetro:

- Activación y configuración de los blades de Identity Awareness, Antivirus, Antibot, IPS y Threat Emulation.

Con la activación del blade de Identity Awareness se conseguirá validar políticas basadas en usuarios de autenticados en el perímetro:

- Identity Awareness:

Habilitar el blade **Identity Awareness**:

a. Seleccionar **AD Query only**.

b. Seleccionar Nuevo dominio: **lab.local**

c. Ingresar con **admin** contraseña **vpn123** y controlador de dominio **192.168.80.80**

d. Presionar **connect** debería de obtener la siguiente respuesta: **Successfully connected!**

e. Dar click dos veces **Next.**.

f. Dar click en **Finish** para completar el wizard.

- IPS:

Se inspeccionará todo el tráfico existente externa, DMZ e interna.

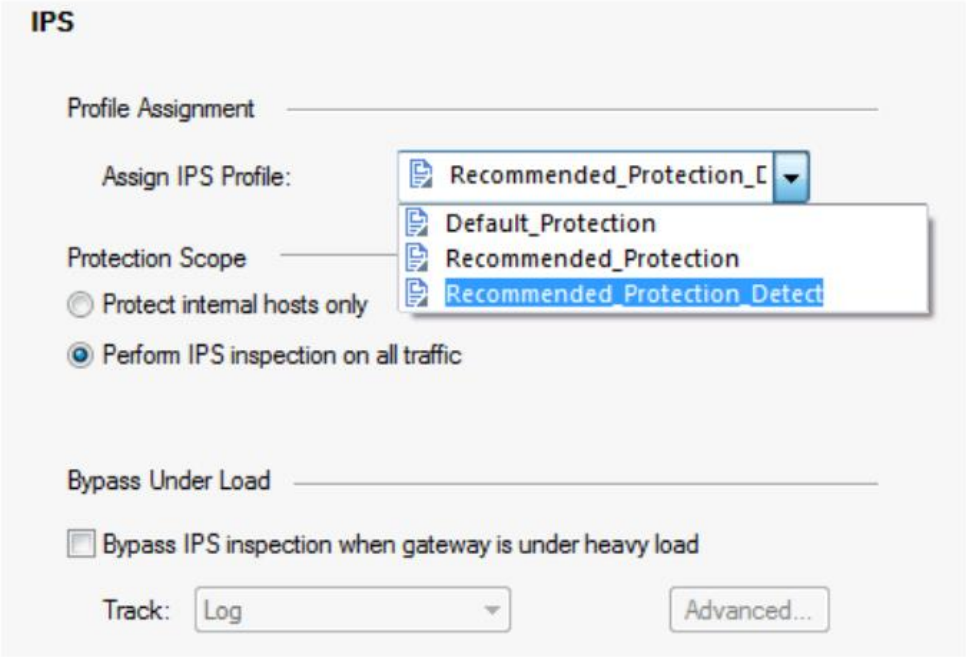


Figura 9: Asignación del IPS Profile en modo detección

- Antivirus y Antibot:

Se hizo la activación de manera automática en el Gateway Check Point como parte de la arquitectura de Threat Prevention.

- Threat Emulation:

Se procedió a activar el blade de Threat Emulation quedando la arquitectura de Threat Prevention de esta manera:

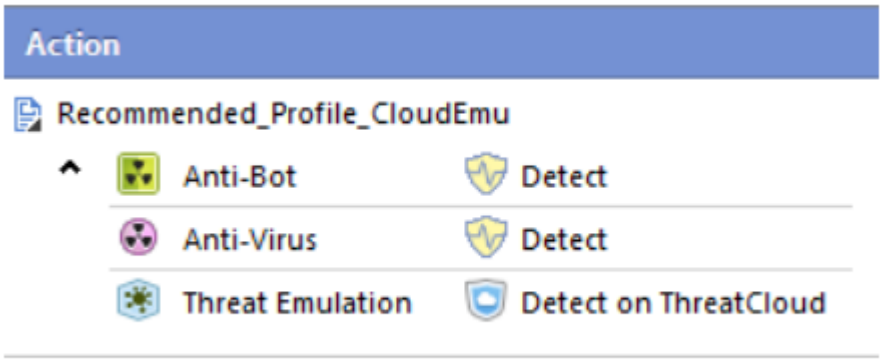


Figura 10: Verificación del Threat Prevention Profile en modo detección

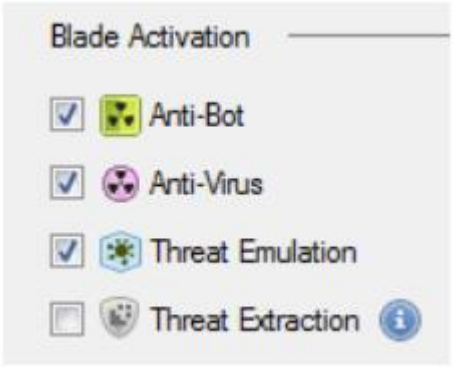


Figura 11: Activación del Anti-Virus, Anti-Bot y Threat Emulation

- Se procedió a configurar el Antivirus:

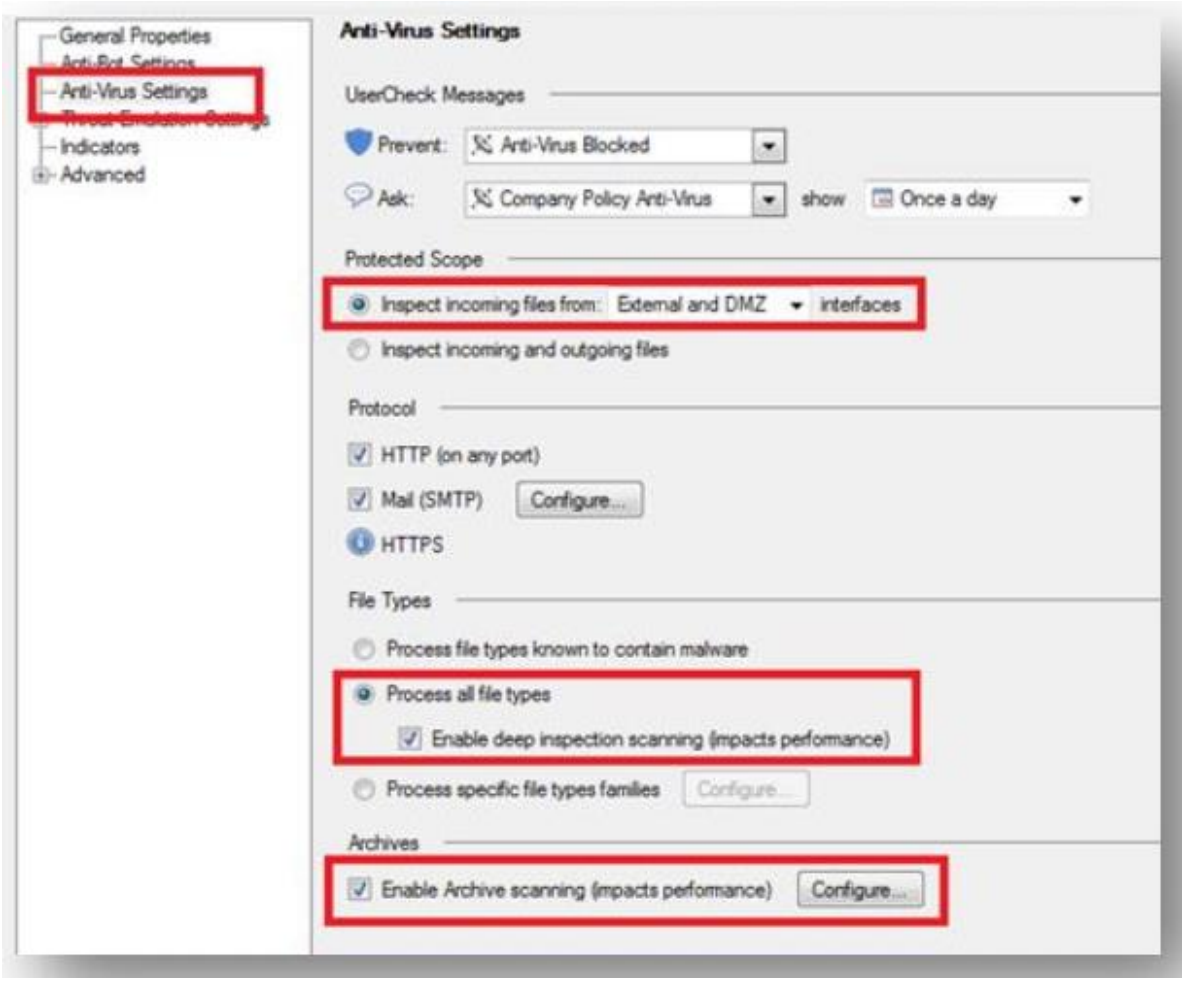


Figura 12: Configuraciones de inspección en el Anti-Virus

Aquí se inspeccionará todo el tráfico entrante de la red externa y hacia la DMZ. El cual el perfil de Threat Prevention estará en esta prueba en modo detección.

Se hizo nuevamente el ataque de comando y control y se validó en el SmartLog del Check Point que sí estaba alarmado de forma crítica por el Antibot e IPS.

Se procedió a ponerlo en modo preventivo.

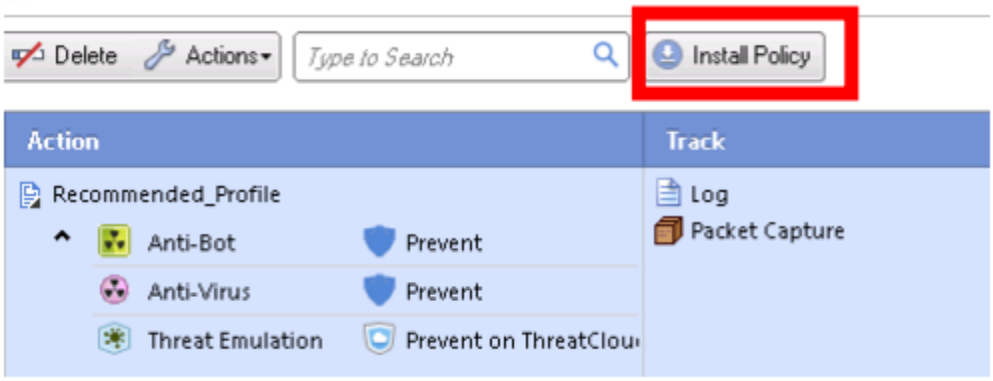


Figura 13: Instalación de políticas Threat Prevention

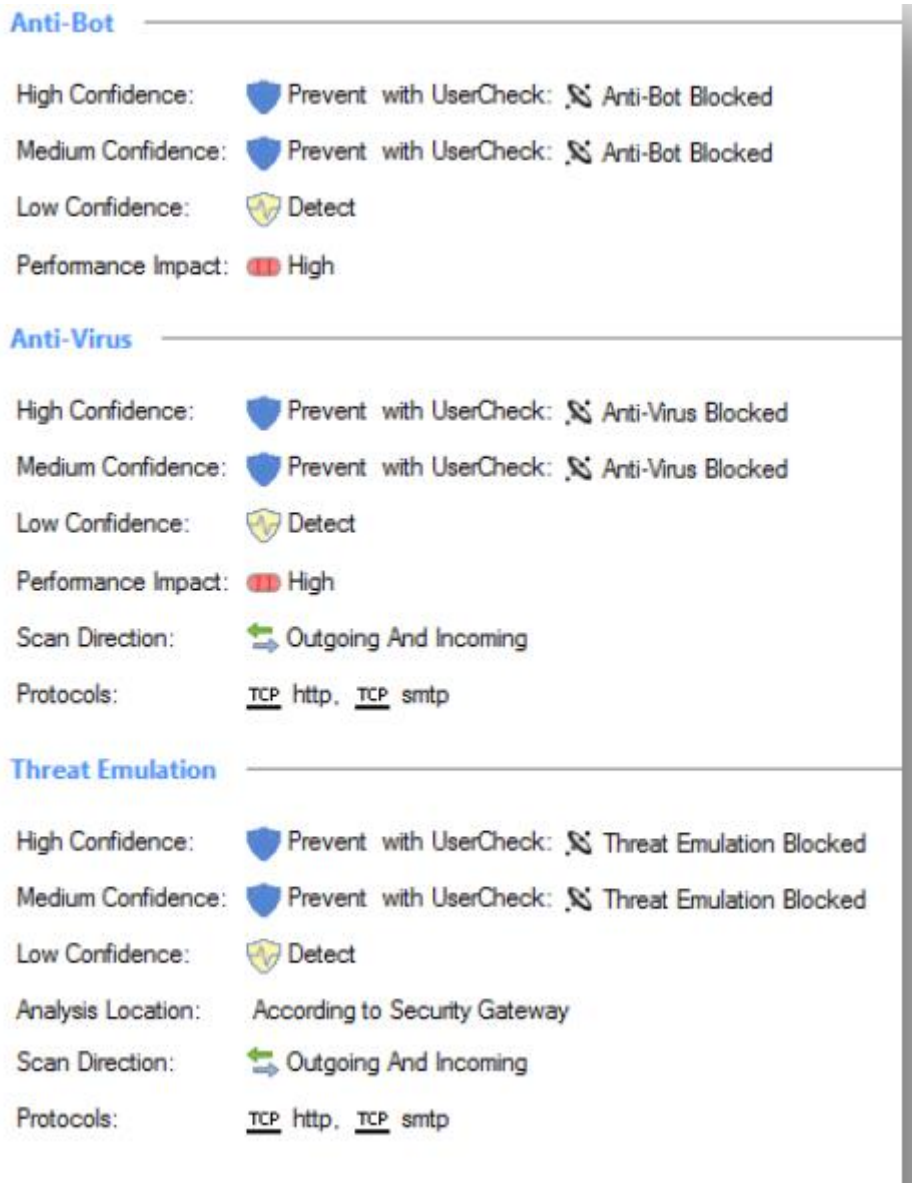


Figura 14: Verificación de Threat Prevention en modo Preventivo

Después del modo de detección a prevención, se hizo nuevamente un análisis en el SmartLog y se ha prevenido ese ataque de comando y control.

- Se procedió a activar y configurar tanto el blade Threat Emulation, como el SmartEvent (Correlación de eventos en tiempo real).

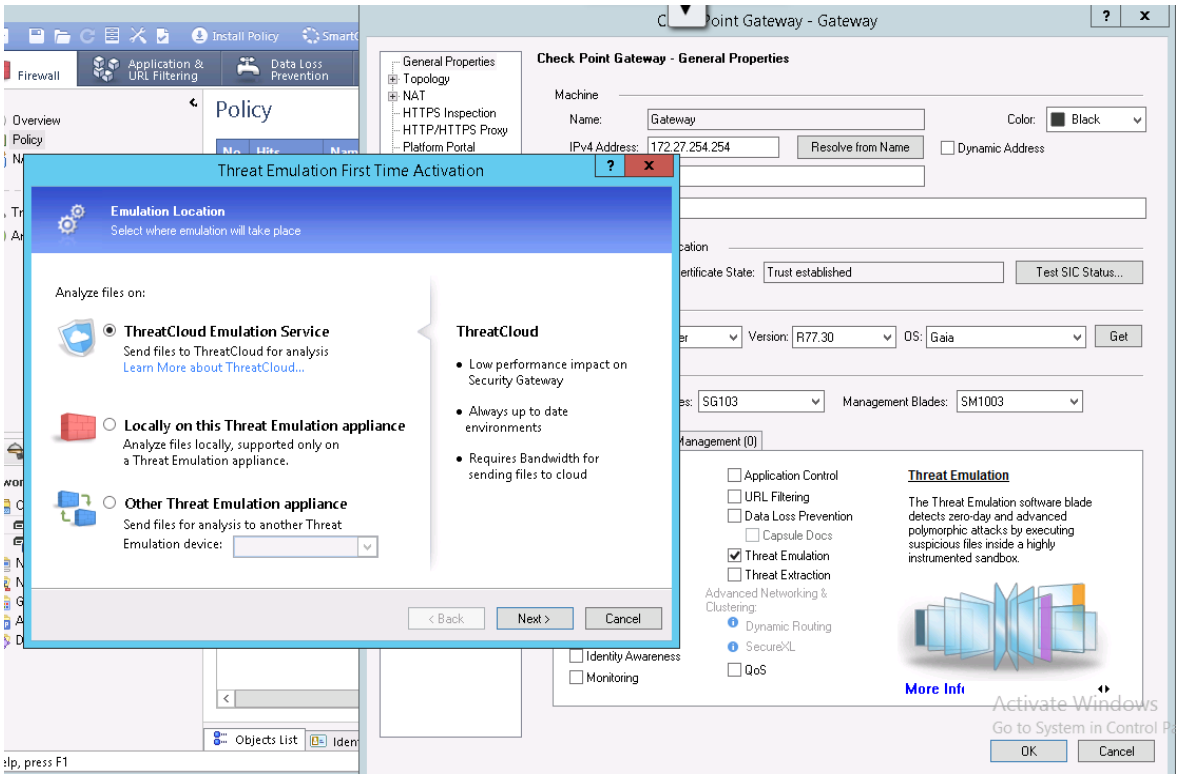


Figura 15: Activación y primera configuración del Threat Emulation Blade

Este método ThreatCloud Emulation Service, se analizará en la nube con la subcripción de la licencia. También a su vez se configuró en deshabilitar análisis estáticos de filtros de archivos.

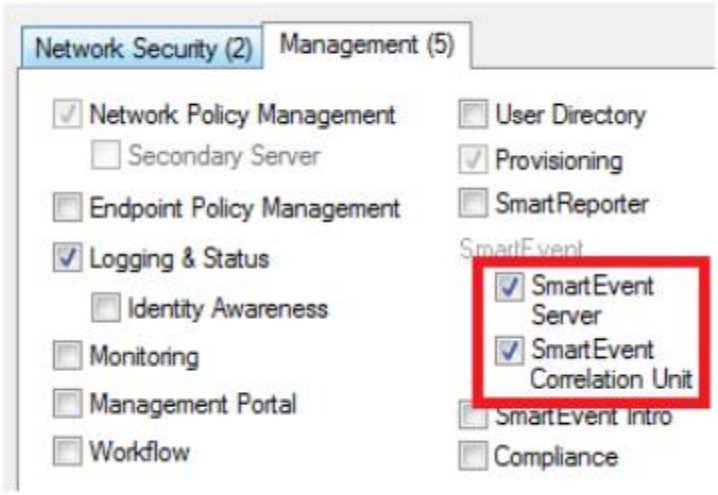


Figura 16: Activación del SmartEvent en Security Management

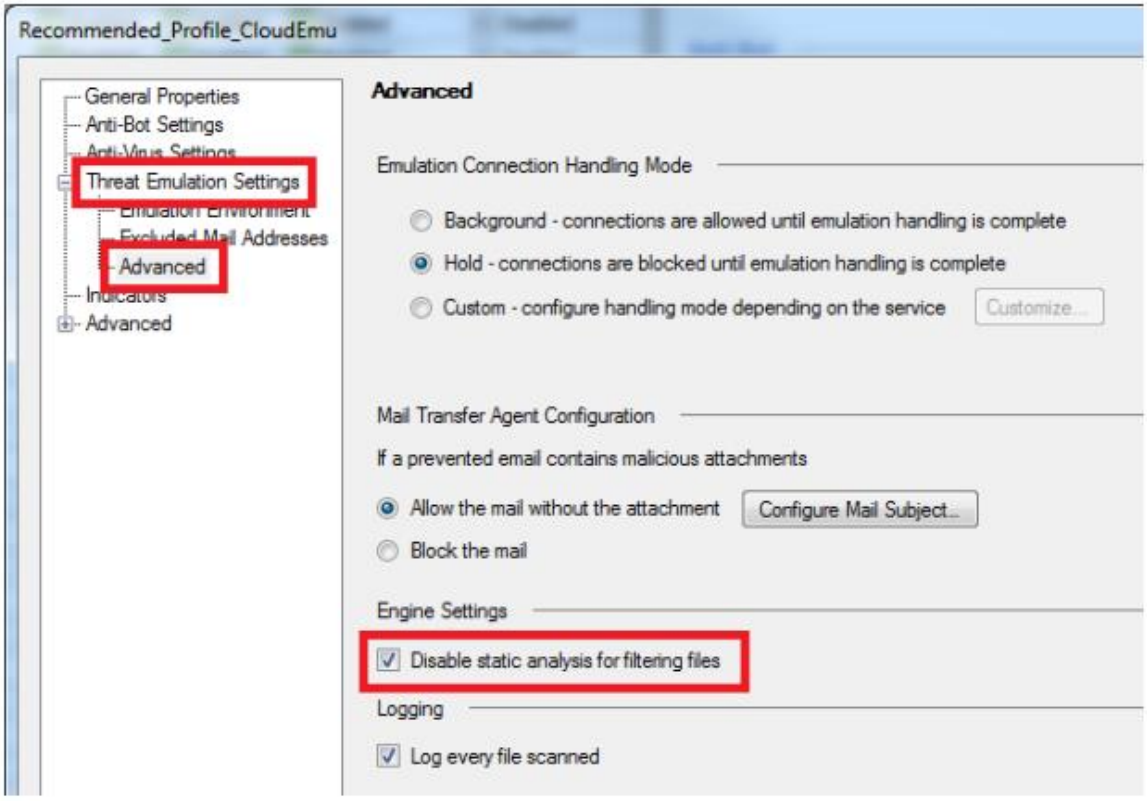


Figura 17: Configuración de la parte avanzada del Threat Emulation

Luego instalamos políticas y validaciones de las suscripciones de la licencia.

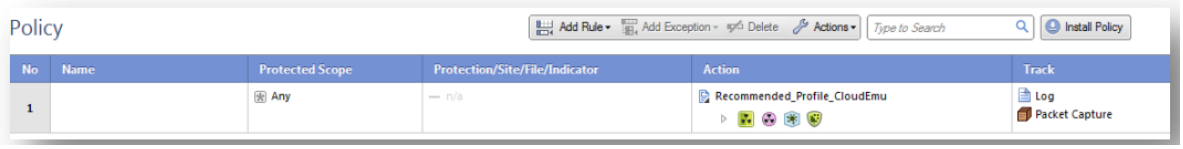


Figura 18: Instalación de políticas en el Threat Prevention

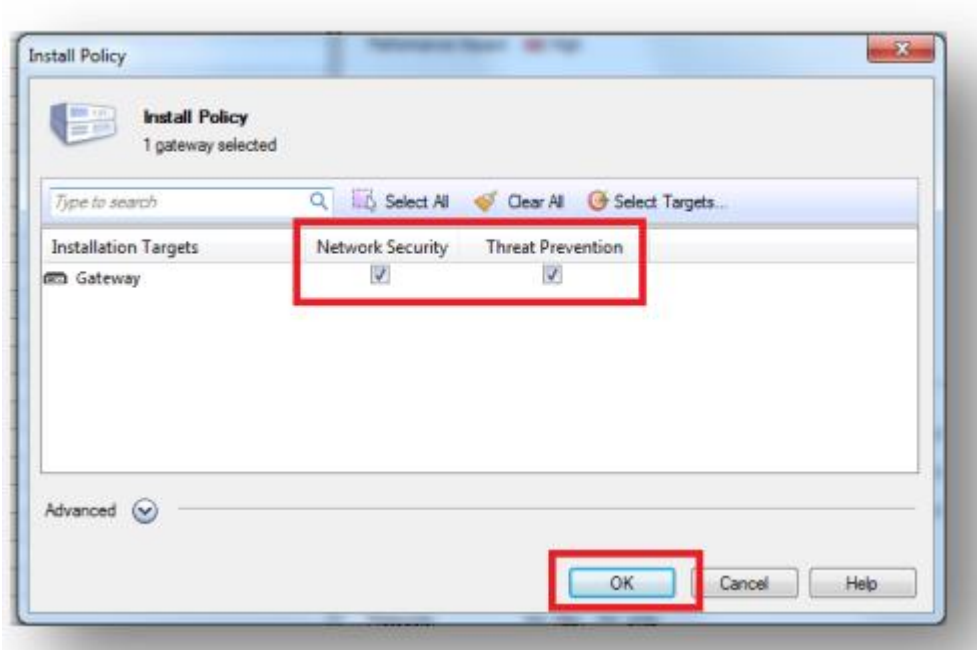


Figura 19: Seleccionando el Gateway para instalar el paquete de políticas

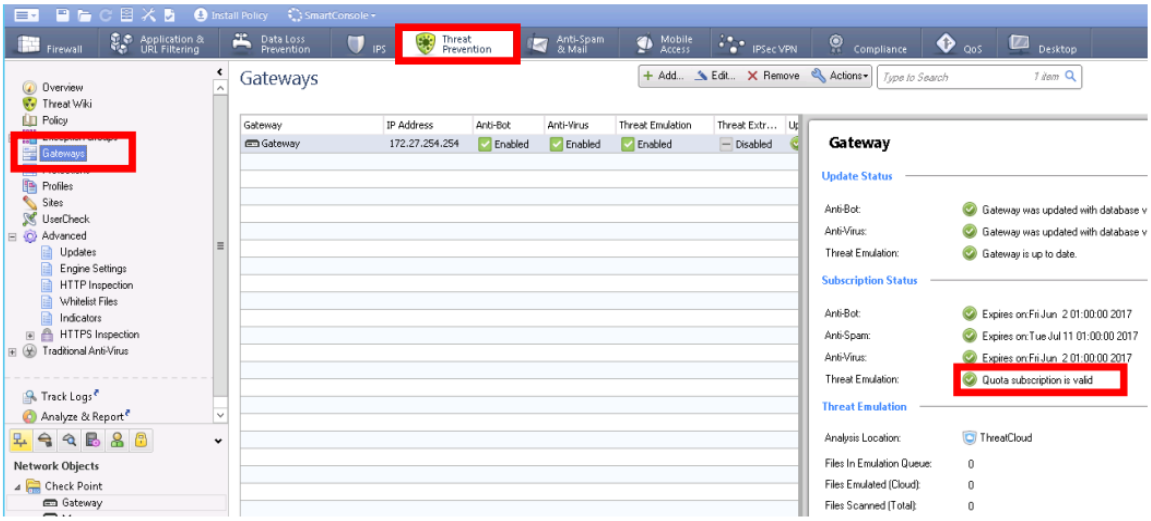


Figura 20: Verificación de la suscripción del Threat Emulation válido

- Proceso de emulación local de archivos maliciosos, en este caso se demostrará el proceso de emulación en tiempo real vía SSH.
    - Habilitar el escaneo de archivos local en el Gateway vía SSH.

```
Gateway> tecli debug scan local enable
Enabling local connection scanning
```

Figura 21: Habilitación de emulación local

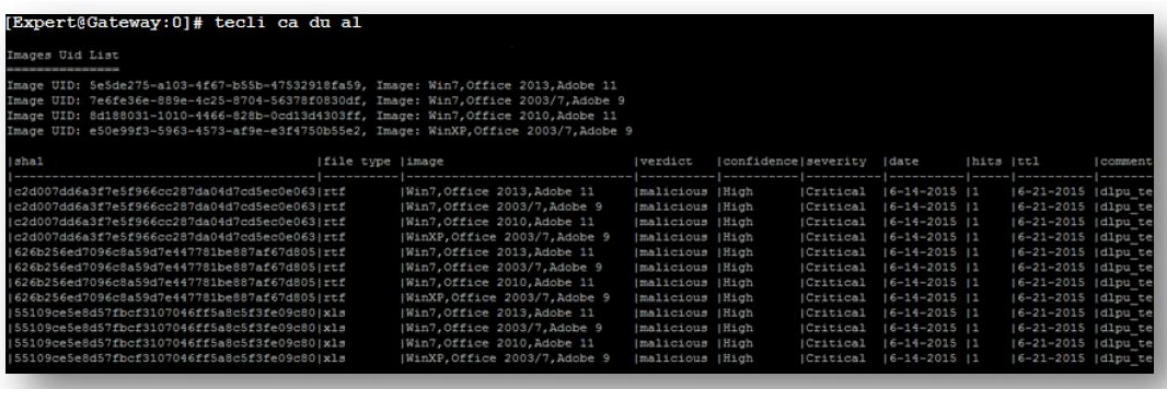
- Habilitar visualización de las emulaciones en cada cierto intervalo de tiempo en el Gateway.

```
watch -d --interval=0.5 "tecli show cloud queue"
```

- Se abrió otra sesion vía SSH al Gateway para ingresar a la carpeta malfiles y ejecutar el archivo getmalfiles.sh.

```
cd malfiles
./getmalfiles.sh
```

- Después que el script se ha ejecutado cierto tiempo vamos a ejecutar el comando **`tecli cache dump all`**, para ver el veredicto y proceso de emulación local.



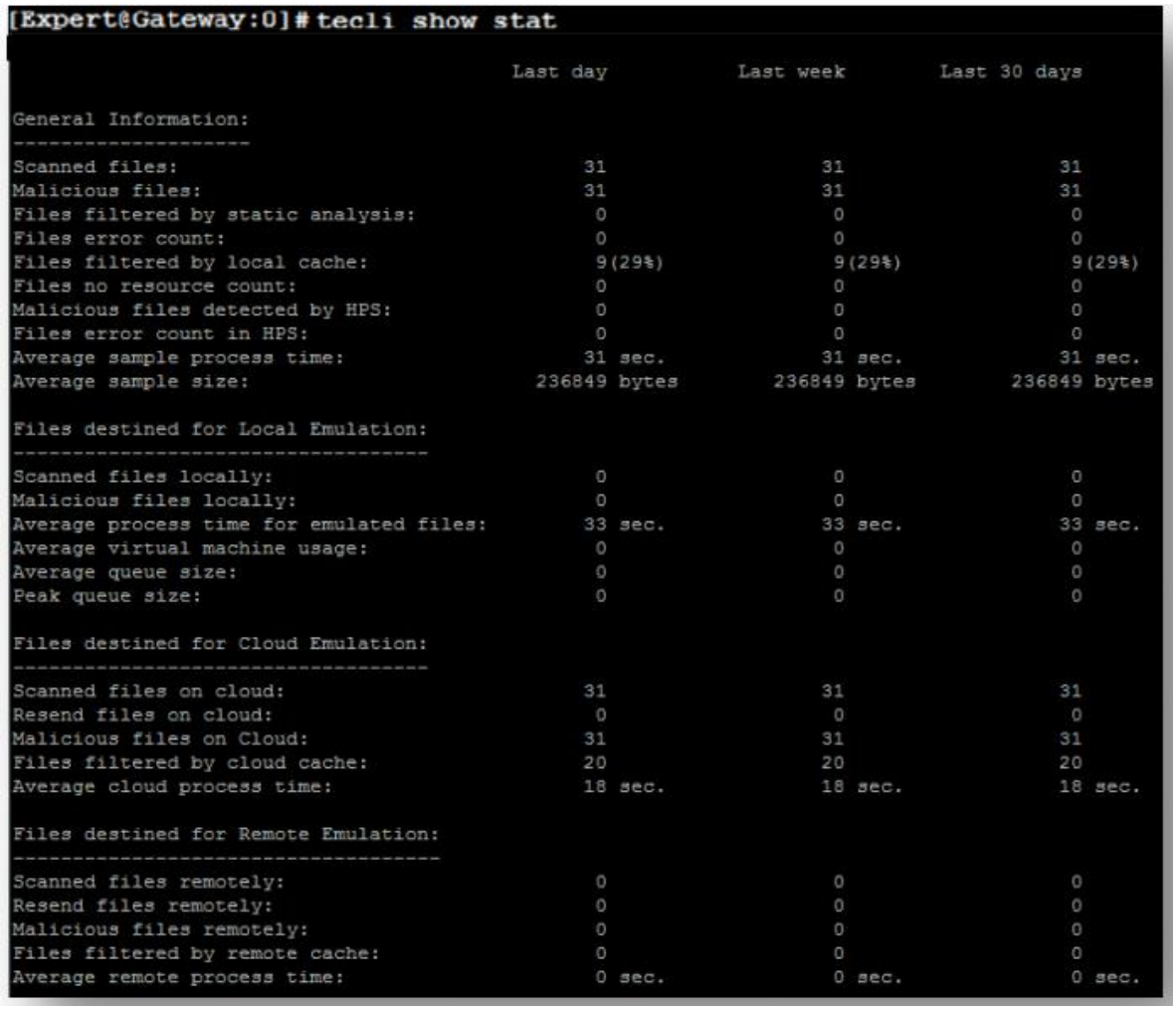
```
[Expert@Gateway:0]# tecli ca du al

Images Uid List
---------------
Image UID: 5e5de275-a103-4f67-b55b-47532918fa59, Image: Win7,Office 2013,Adobe 11
Image UID: 7e6fe36e-889e-4c25-8704-56378f0830df, Image: Win7,Office 2003/7,Adobe 9
Image UID: 8d188031-1010-4466-828b-0cd13d4303ff, Image: Win7,Office 2010,Adobe 11
Image UID: e50e99f3-5963-4573-af9e-e3f4750b55e2, Image: WinXP,Office 2003/7,Adobe 9

|sha1                                     |file type |image                          |verdict   |confidence|severity  |date      |hits |ttl       |comment
|-----------------------------------------|----------|-------------------------------|----------|----------|----------|----------|-----|----------|-------
|c2d007dd6a3f7e5f966cc287da04d7cd5ec0e063|rtf       |Win7,Office 2013,Adobe 11      |malicious |High      |Critical  |6-14-2015 |1    |6-21-2015 |dlpu_te
|c2d007dd6a3f7e5f966cc287da04d7cd5ec0e063|rtf       |Win7,Office 2003/7,Adobe 9     |malicious |High      |Critical  |6-14-2015 |1    |6-21-2015 |dlpu_te
|c2d007dd6a3f7e5f966cc287da04d7cd5ec0e063|rtf       |Win7,Office 2010,Adobe 11      |malicious |High      |Critical  |6-14-2015 |1    |6-21-2015 |dlpu_te
|c2d007dd6a3f7e5f966cc287da04d7cd5ec0e063|rtf       |WinXP,Office 2003/7,Adobe 9    |malicious |High      |Critical  |6-14-2015 |1    |6-21-2015 |dlpu_te
|626b256ed7096c8a59d7e447781be887af67d805|rtf       |Win7,Office 2013,Adobe 11      |malicious |High      |Critical  |6-14-2015 |1    |6-21-2015 |dlpu_te
|626b256ed7096c8a59d7e447781be887af67d805|rtf       |Win7,Office 2003/7,Adobe 9     |malicious |High      |Critical  |6-14-2015 |1    |6-21-2015 |dlpu_te
|626b256ed7096c8a59d7e447781be887af67d805|rtf       |Win7,Office 2010,Adobe 11      |malicious |High      |Critical  |6-14-2015 |1    |6-21-2015 |dlpu_te
|626b256ed7096c8a59d7e447781be887af67d805|rtf       |WinXP,Office 2003/7,Adobe 9    |malicious |High      |Critical  |6-14-2015 |1    |6-21-2015 |dlpu_te
|55109ce5e8d57fbcf3107046ff5a8c5f3fe09c80|xls       |Win7,Office 2013,Adobe 11      |malicious |High      |Critical  |6-14-2015 |1    |6-21-2015 |dlpu_te
|55109ce5e8d57fbcf3107046ff5a8c5f3fe09c80|xls       |Win7,Office 2003/7,Adobe 9     |malicious |High      |Critical  |6-14-2015 |1    |6-21-2015 |dlpu_te
|55109ce5e8d57fbcf3107046ff5a8c5f3fe09c80|xls       |Win7,Office 2010,Adobe 11      |malicious |High      |Critical  |6-14-2015 |1    |6-21-2015 |dlpu_te
|55109ce5e8d57fbcf3107046ff5a8c5f3fe09c80|xls       |WinXP,Office 2003/7,Adobe 9    |malicious |High      |Critical  |6-14-2015 |1    |6-21-2015 |dlpu_te
```

Figura 22: Visualización de veredicto según la emulación del archivo

- Luego se visualiza las estadísticas de las emulaciones tanto Cloud y local.



```
[Expert@Gateway:0]# tecli show stat

                                    Last day          Last week        Last 30 days

General Information:
--------------------
Scanned files:                            31                 31                  31
Malicious files:                          31                 31                  31
Files filtered by static analysis:         0                  0                   0
Files error count:                         0                  0                   0
Files filtered by local cache:             9(29%)             9(29%)              9(29%)
Files no resource count:                   0                  0                   0
Malicious files detected by HPS:           0                  0                   0
Files error count in HPS:                  0                  0                   0
Average sample process time:              31 sec.            31 sec.             31 sec.
Average sample size:                  236849 bytes       236849 bytes        236849 bytes

Files destined for Local Emulation:
-----------------------------------
Scanned files locally:                     0                  0                   0
Malicious files locally:                   0                  0                   0
Average process time for emulated files:  33 sec.            33 sec.             33 sec.
Average virtual machine usage:             0                  0                   0
Average queue size:                        0                  0                   0
Peak queue size:                           0                  0                   0

Files destined for Cloud Emulation:
-----------------------------------
Scanned files on cloud:                   31                 31                  31
Resend files on cloud:                     0                  0                   0
Malicious files on Cloud:                 31                 31                  31
Files filtered by cloud cache:            20                 20                  20
Average cloud process time:               18 sec.            18 sec.             18 sec.

Files destined for Remote Emulation:
------------------------------------
Scanned files remotely:                    0                  0                   0
Resend files remotely:                     0                  0                   0
Malicious files remotely:                  0                  0                   0
Files filtered by remote cache:            0                  0                   0
Average remote process time:               0 sec.             0 sec.              0 sec.
```

Figura 23: Visualización de las estadísticas de las emulaciones realizadas

- Se procedió a validar el reporte forense mediante el SmartView Tracker y SmartLog.

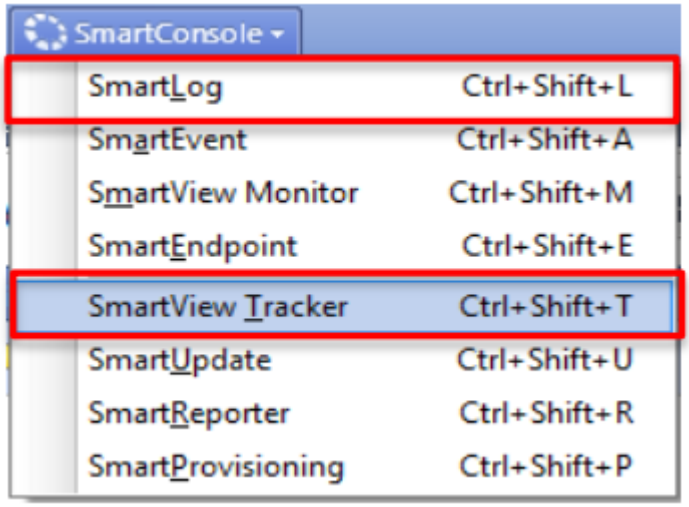


Figura 24: Seleccionando los visualizadores de Logs avanzados

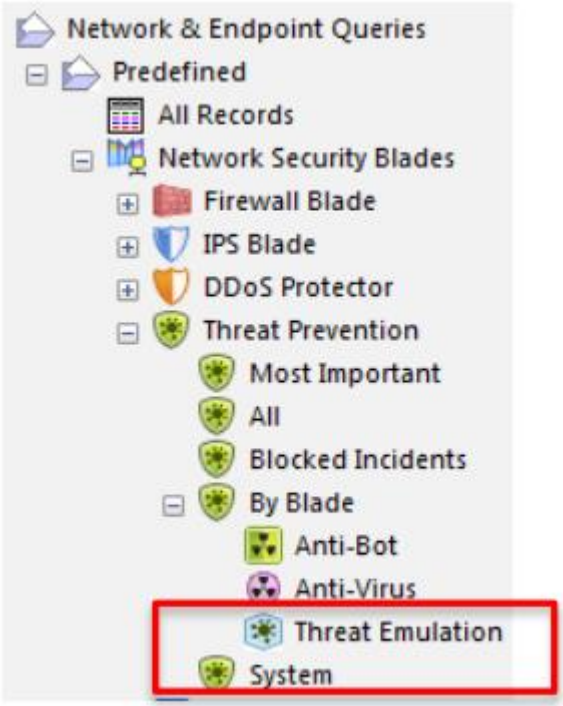


Figura 25: Seleccionando el blade de Threat Emulation para ver los Logs

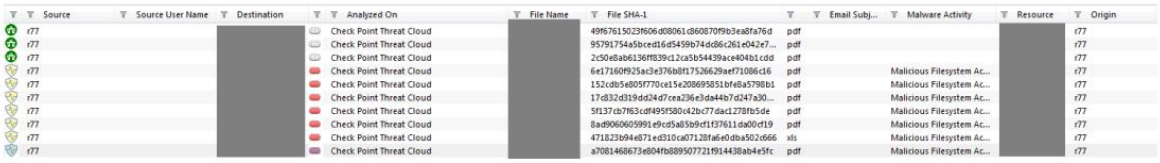


Figura 26: Detección crítico del ataque

La emulación se tiene en modo detección y notamos que ha encontrado archivos de veredictos críticos.

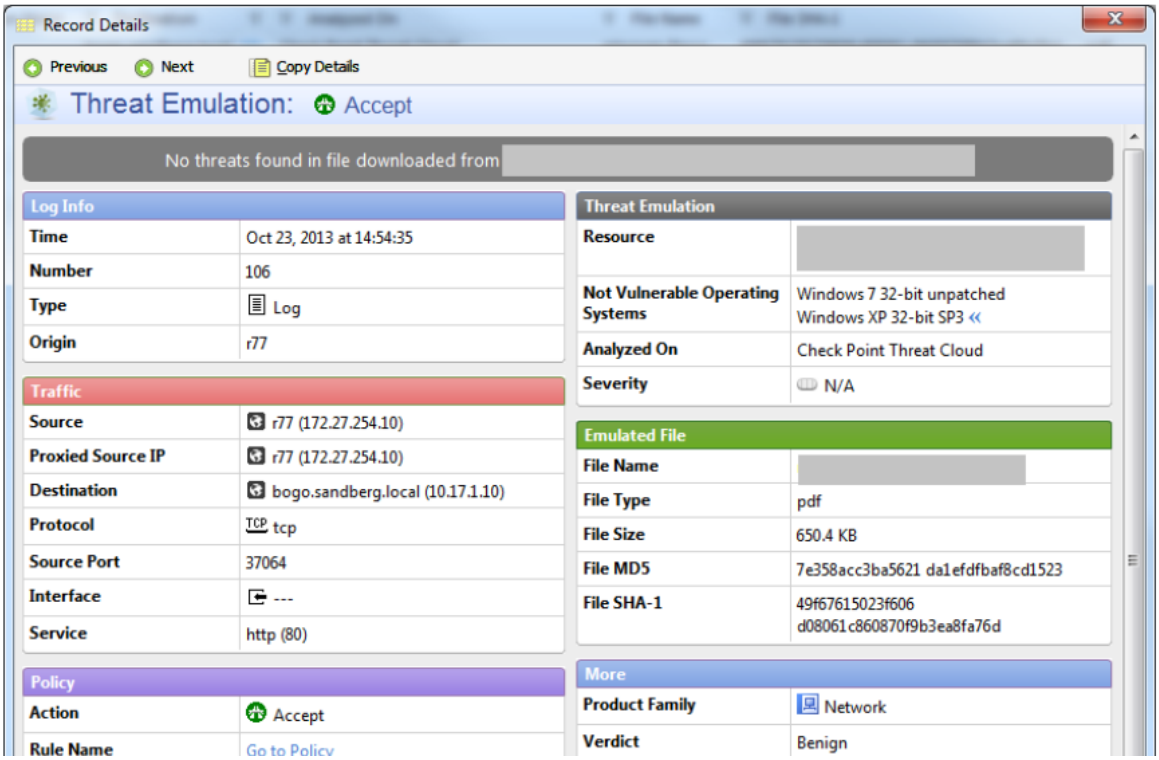


Figura 27: Análisis del Log no infectado

Esta es un Log de archivos no infectados como ejemplo.

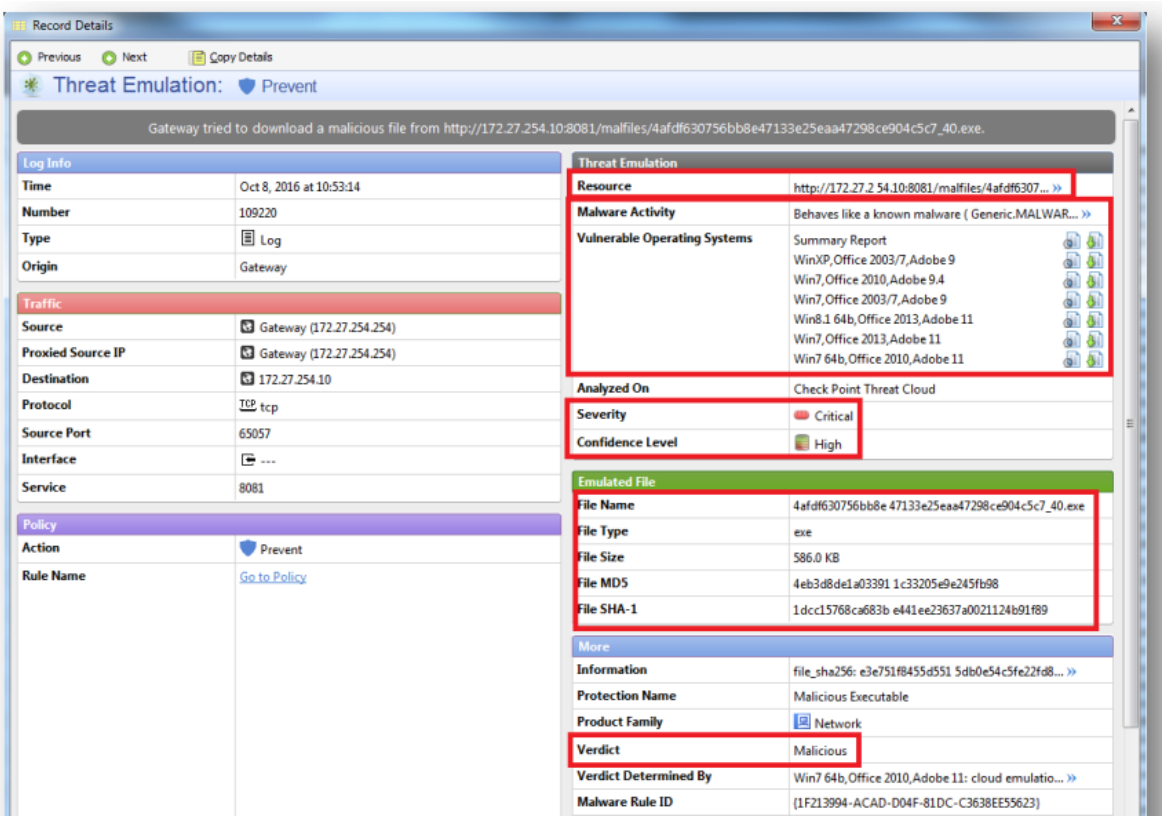


Figura 28: Análisis completo del Log infectado

Este es un Log de tipo malicioso, donde se tiene un reporte tanto en Word o PDF para visualizar directamente con el SmartEvent de cómo y qué hace el Malware dentro del Sandblast.

Reporte:

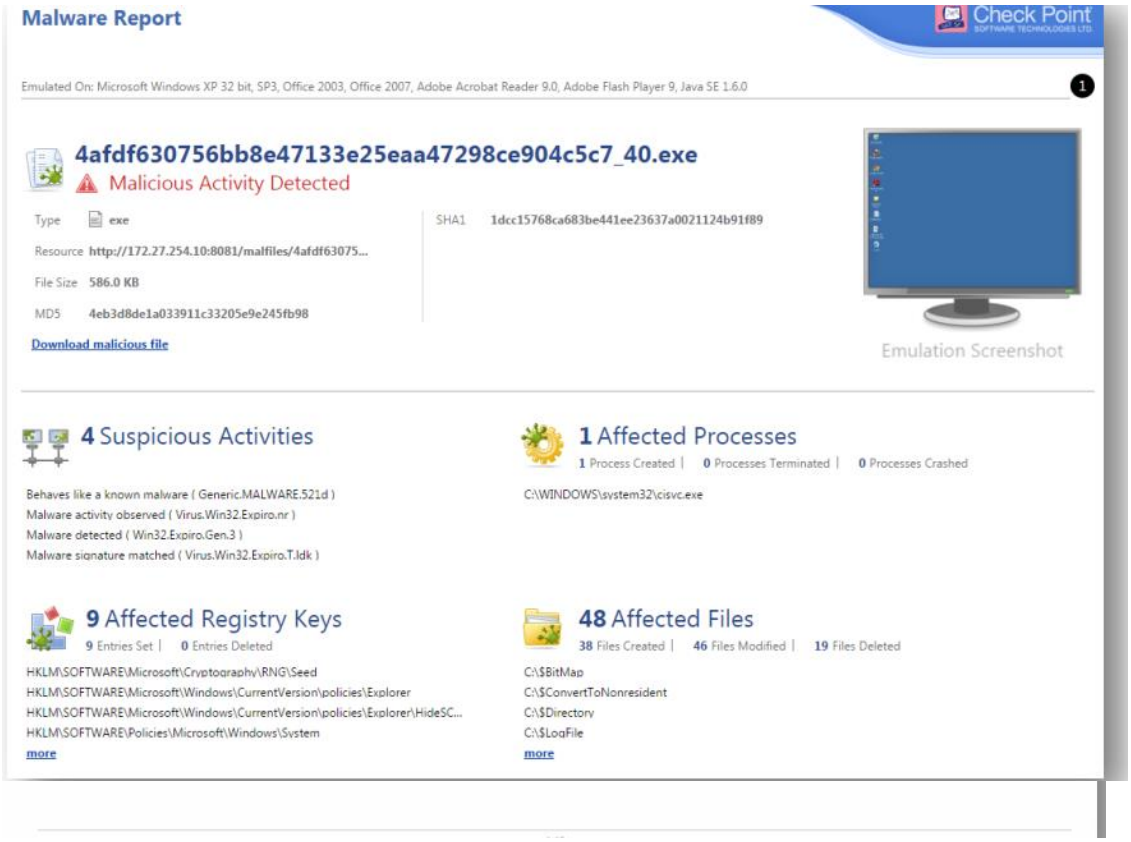


Figura 29: Reporte del Log infectado parte 1

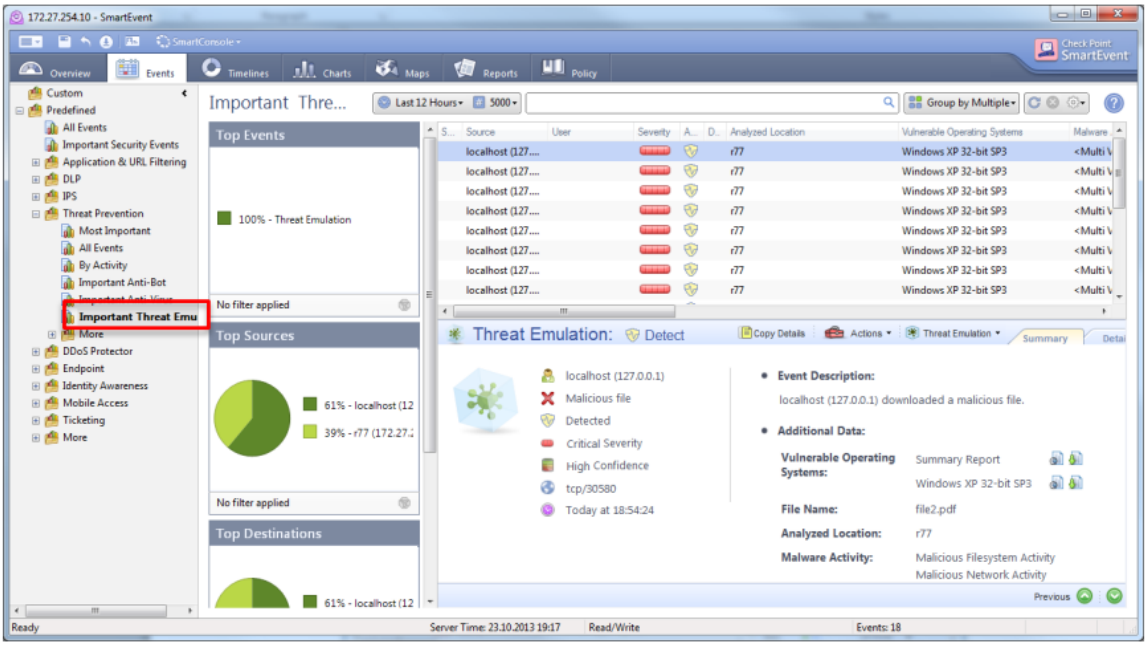


Figura 30: Reporte del Log infectado parte 2

Directamente reports generados desde el SmartEvent

Figura 31: Visualización del evento malicioso detectado en el SmartEvent parte 1

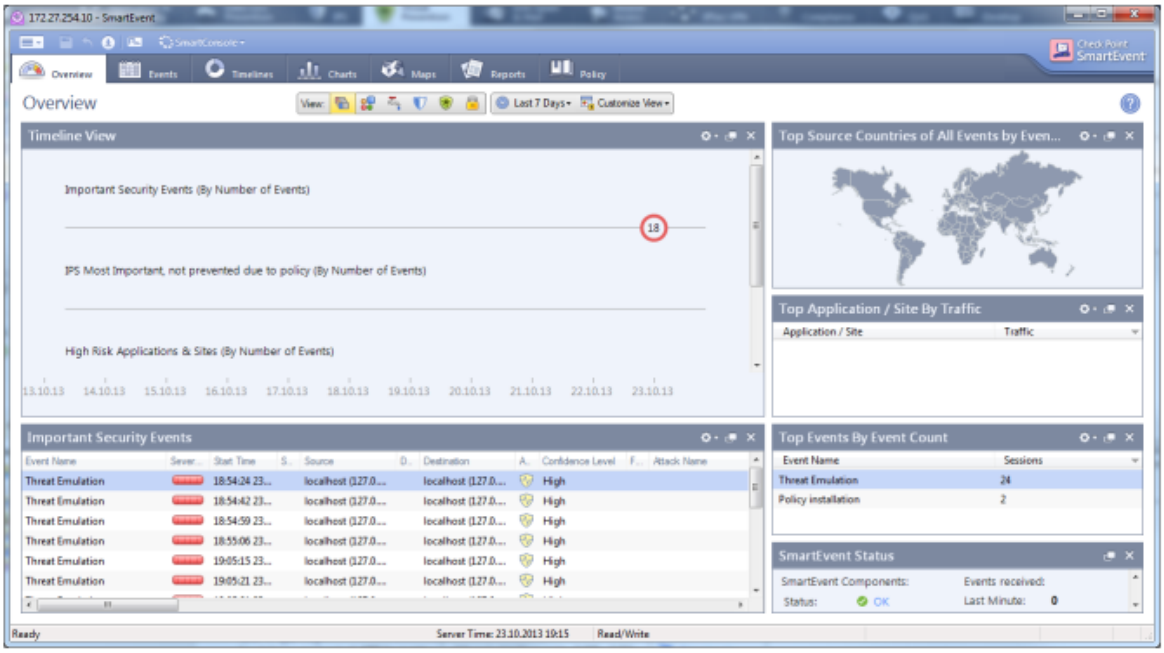


Figura 32: Visualización del evento malicioso detectado en el SmartEvent parte 2

Se puede generar un programador de ejecuciones de reportes.

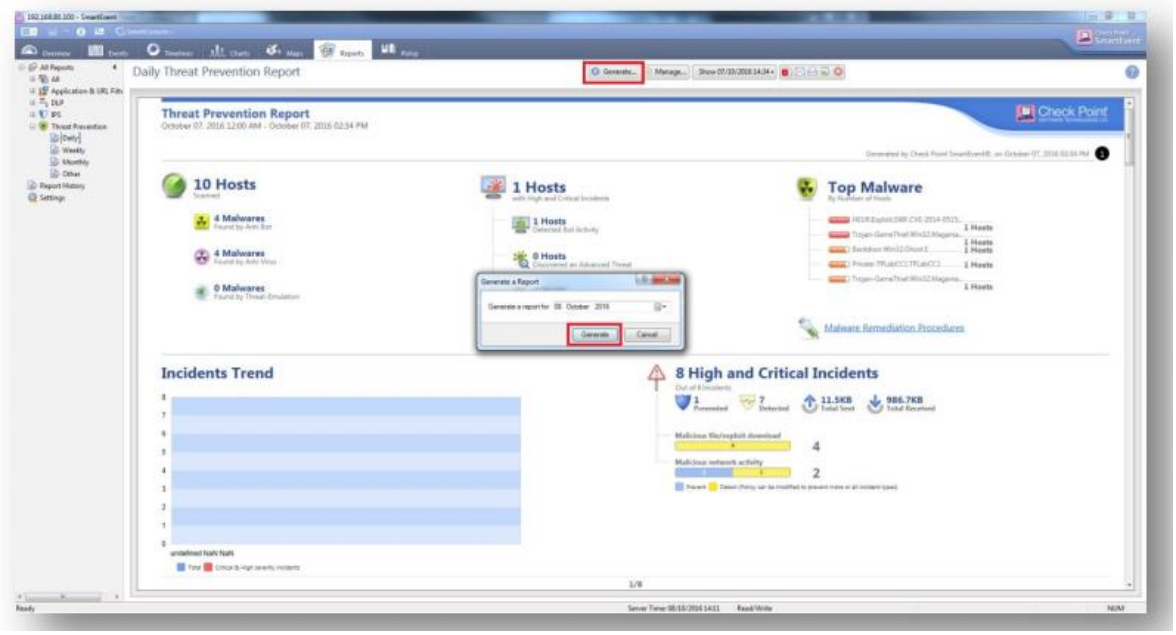


Figura 33: Generando el reporte del malware

- Emulación Local con tráfico de tipo SMTP mediante MTA y se procedió a configurar el MTA en el Check Point.

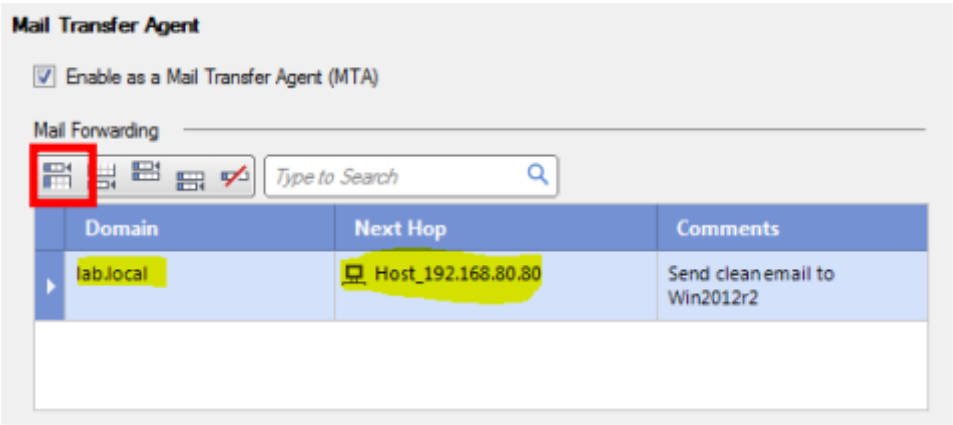


Figura 34: Habilitando el Inline mode vía MTA

Se ha mandado el tráfico SMTP Relay al Servidor 192.168.80.80 y se procedió a configurar el cliente SMTP en la máquina de Jlennon.

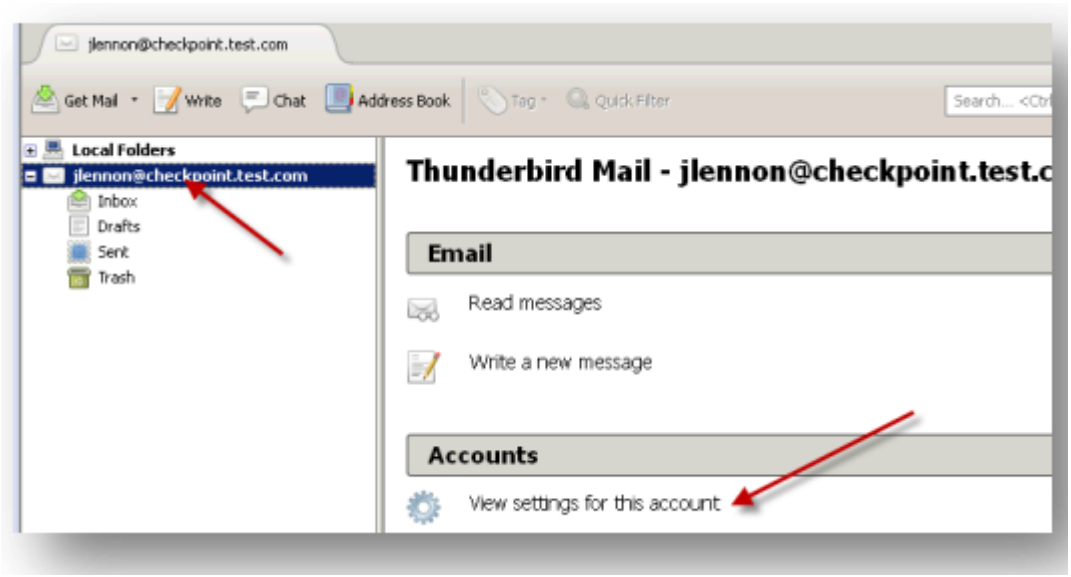


Figura 35: Configuración del cliente de correo

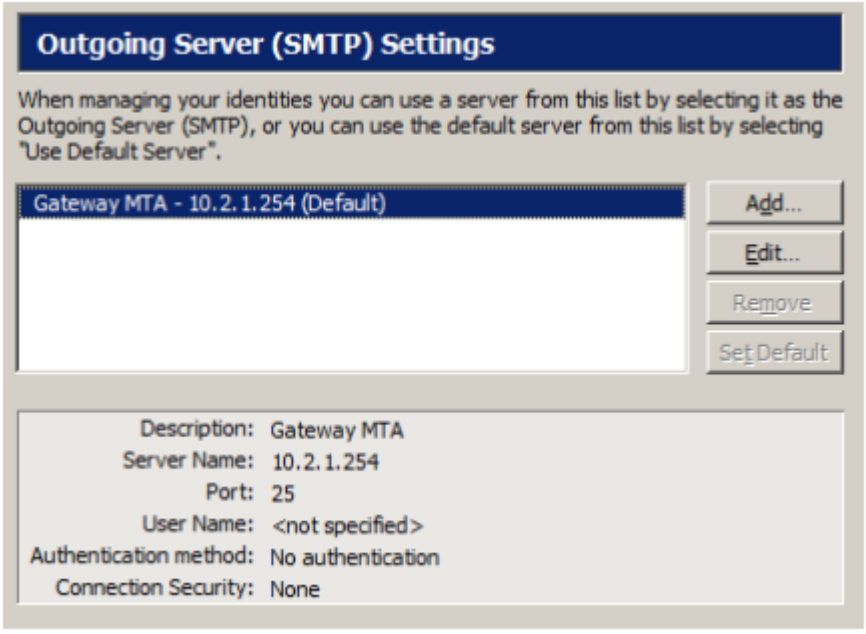


Figura 36: Configuración del cliente SMTP saliente

Se va a hacer pruebas en modo MTA Inline la emulación local.

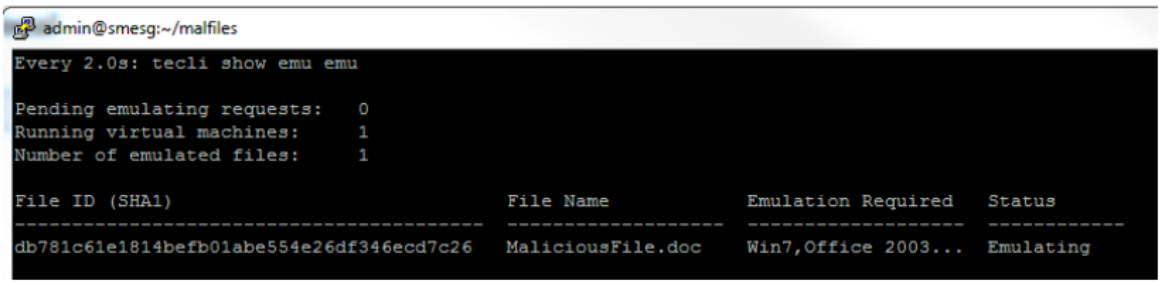


Figura 37: Visualización de la emulación cada 2 segundos

En ese momento el cliente recibe un correo con que el archivo es malicioso.

Figura 38: Correo del mensaje del archivo malicioso

- Habilitar Threat Extraction SMTP Inline vía MTA:

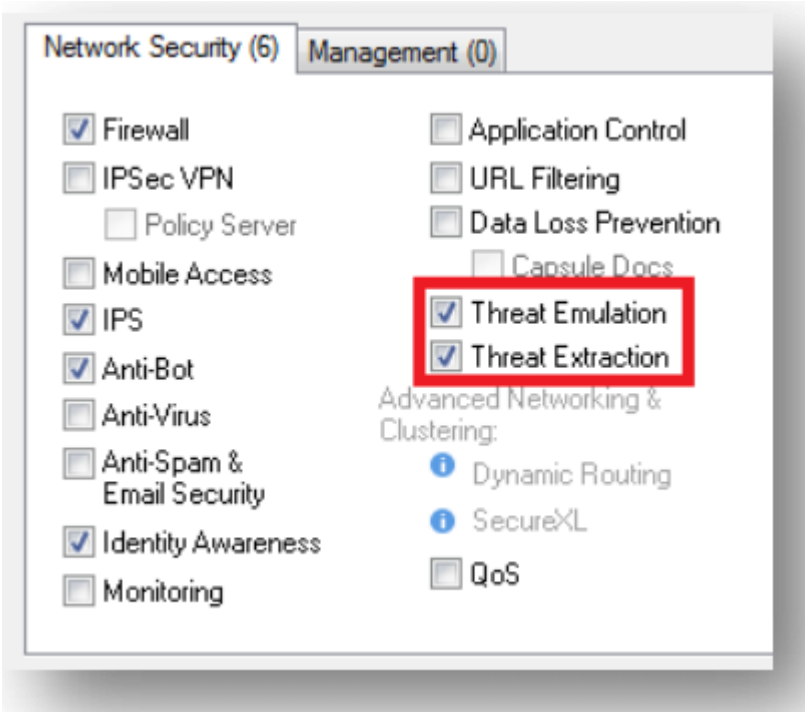


Figura 39: Activando Threat Extraction Inline Mode vía MTA

De manera que se activará en el Gateway y se configurará en el Threat Prevention Profile en modo Clean.

Figura 40: Threat Extraction en modo limpieza manteniendo el formato original

Se validará si ya se tiene el MTA habilitado y si no, este sería la primera vez que se active el Threat Extraction.

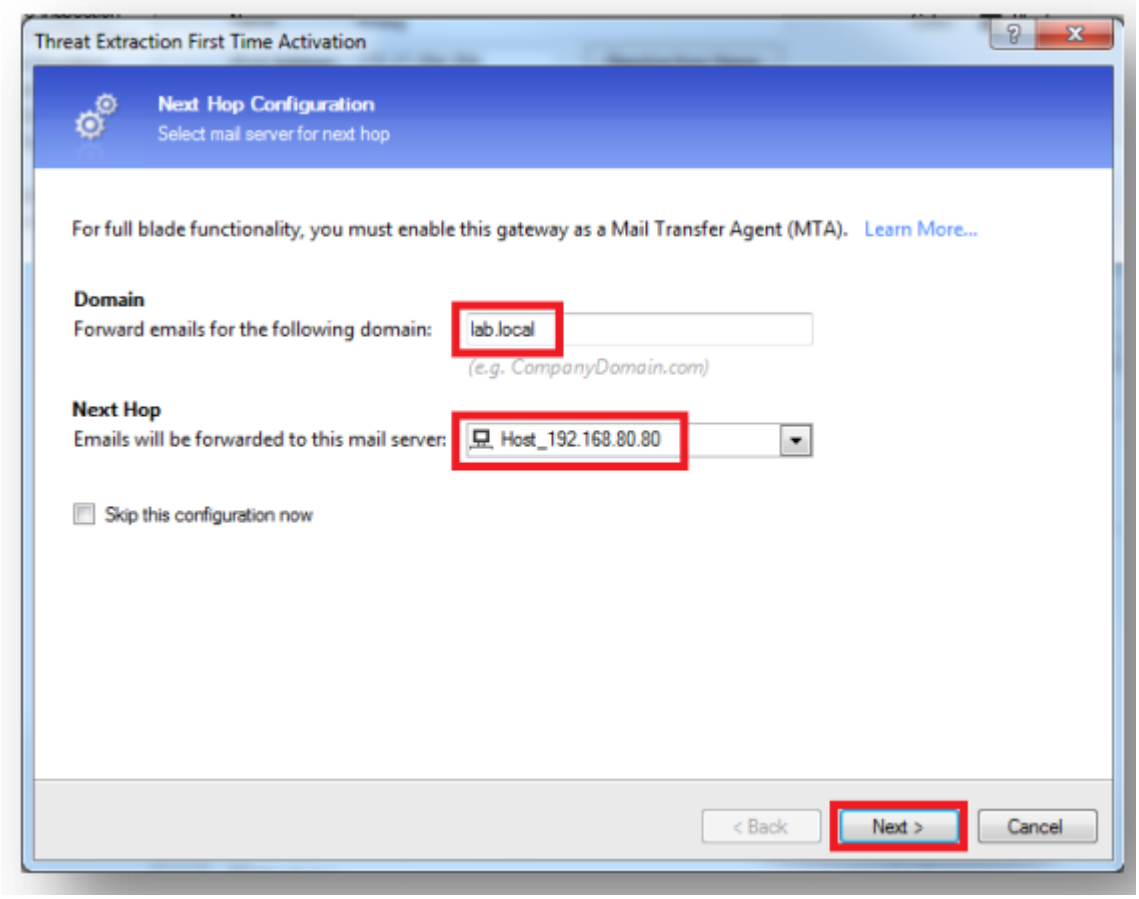


Figura 41: configurando el MTA Inline con Threat Extraction del dominio lab.local

Se procederá a configurar el perfil del Threat Extraction para convertir el archivo en PDF o mantener el formato original.

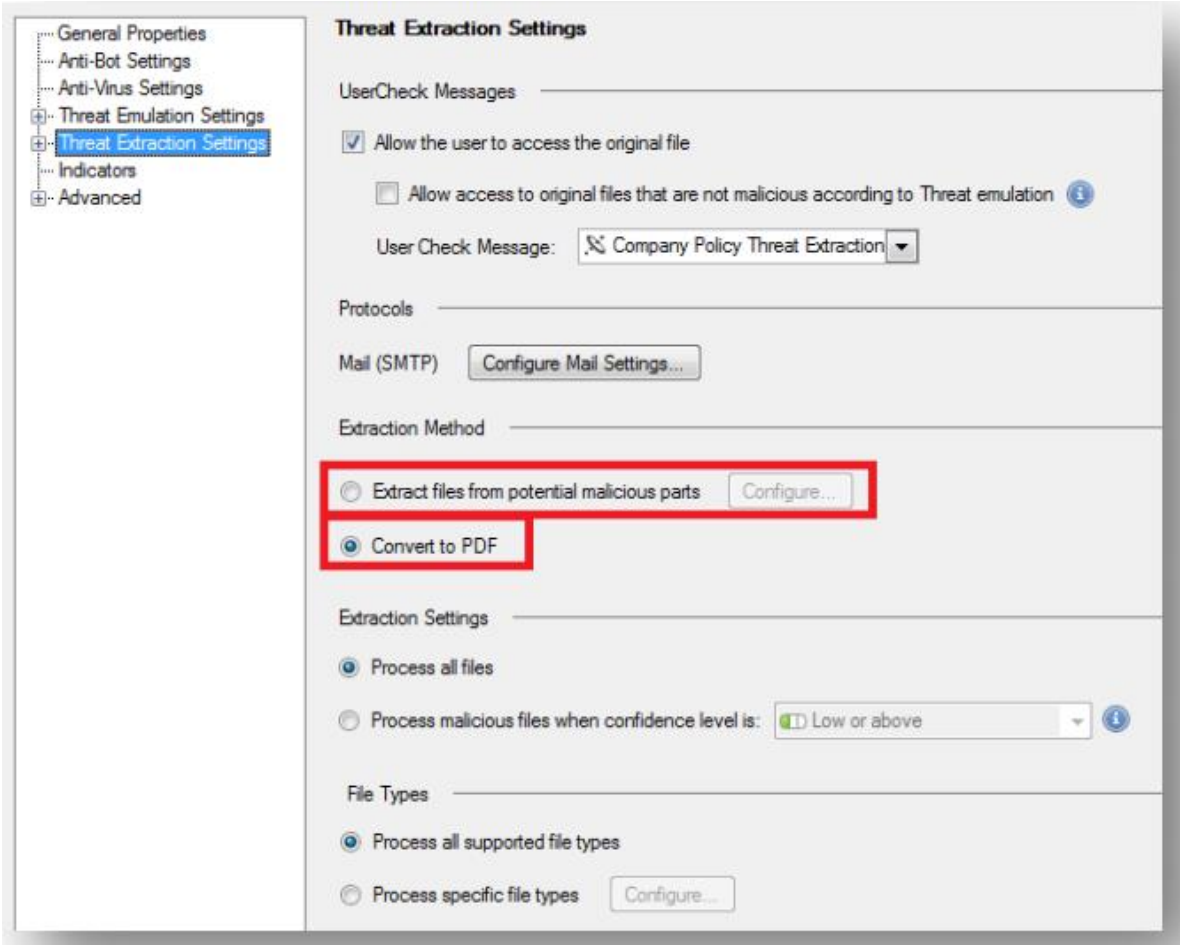


Figura 42: Métodos de Extracción de archivos

Se realizará la misma prueba con el cliente al enviar el mismo archivo malicioso pero esta vez pasará el archivo por Threat Extraction, convirtiendo el archivo en PDF limpio y el archivo original se estará emulando mientras tanto el cliente tendrá el archivo en limpio de manera seguro vía MTA, mejorando el rendimiento de manera segura y eficaz en Sandblast.

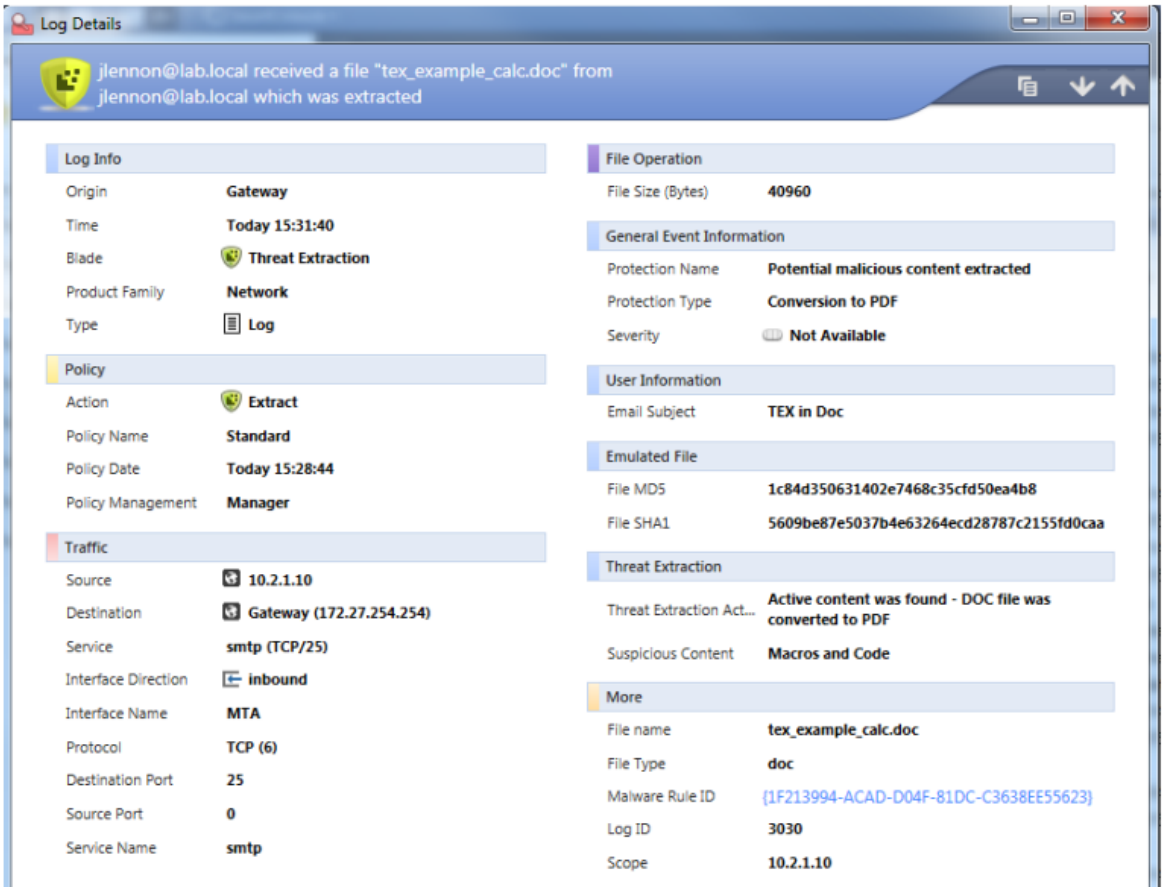
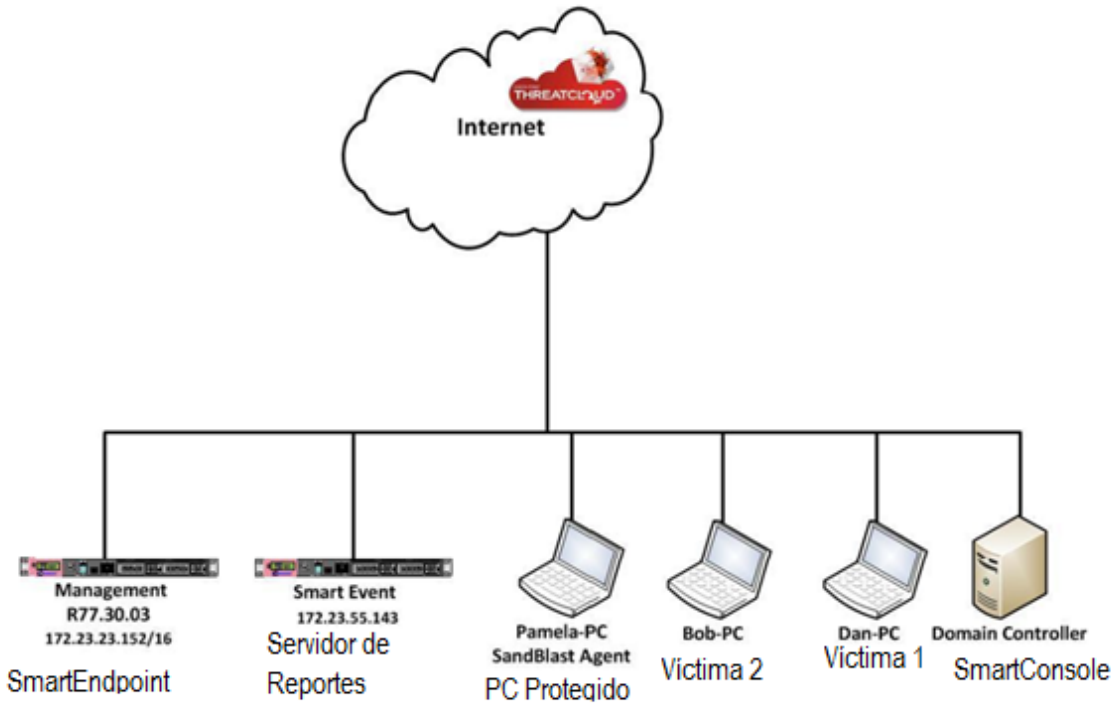


Figura 43: Análisis de Logs malicioso con Threat Extraction

Se hizo nuevamente el análisis en el SmartLog y se hizo la extracción del Malware de manera segura hacia el cliente.

4.2 Configuración y despliegue de Sandblast Agent:

TopologSandblast Agent



Dentro de las configuraciones del Sandblast Agent se tiene configurado lo siguiente:

Check Point Security Management en R77.30.03, la versión que ofrece el Sandblast Agent mediante el SmartEndpoint.

- Despliegue del Sandblast Agent en la maquina víctima:

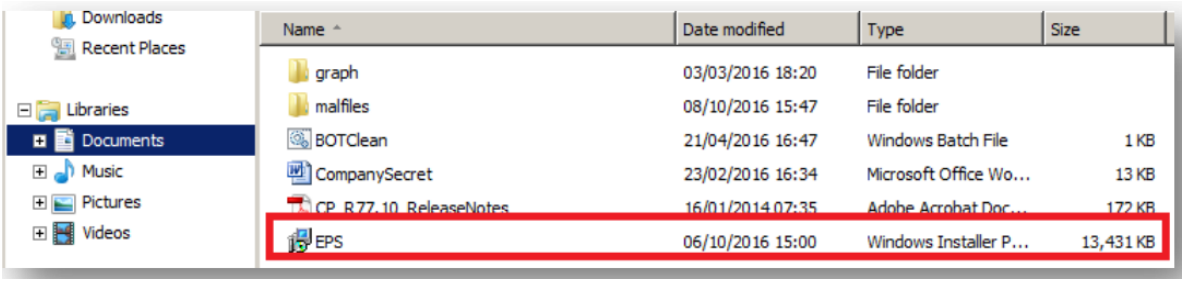


Figura 44: Instalación del Sandblast Agent en la máquina víctima

- Se hará inicio de sesión en el SmartEndpoint.

Figura 45: Inicio de sesión en la consola de SmartEndpoint

- Dentro de la consola administrativa del Endpoint se hará una nueva regla para la máquina víctima 2.

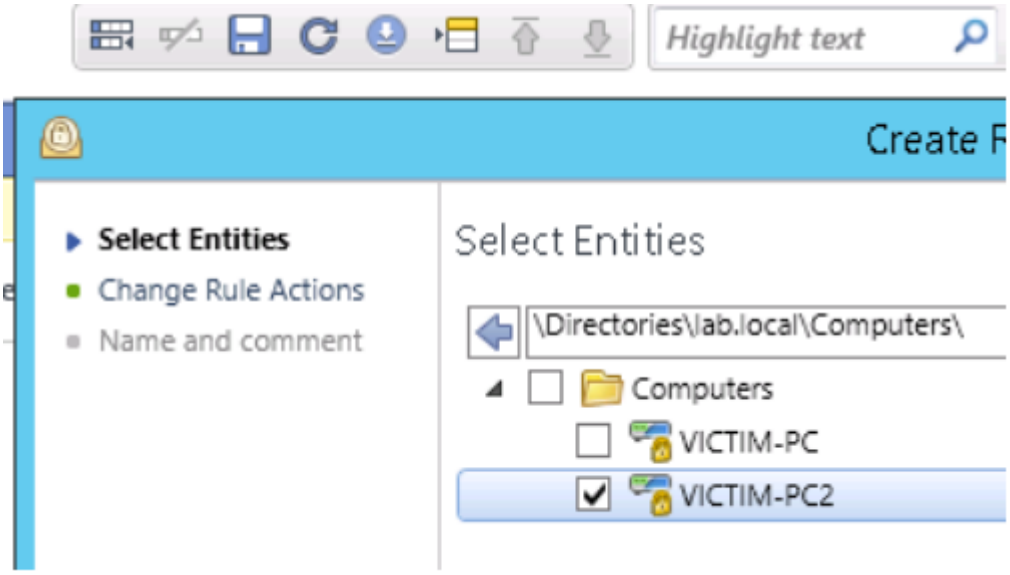


Figura 46: Creación de una nueva política para la máquina victima

- Se hizo un escaneo para enviarle las políticas.

Figura 47: Activando Threat Extraction Inline Mode vía MTA

- Se hizo las configuraciones de emulación y extracción en la nube, y luego instalamos políticas.

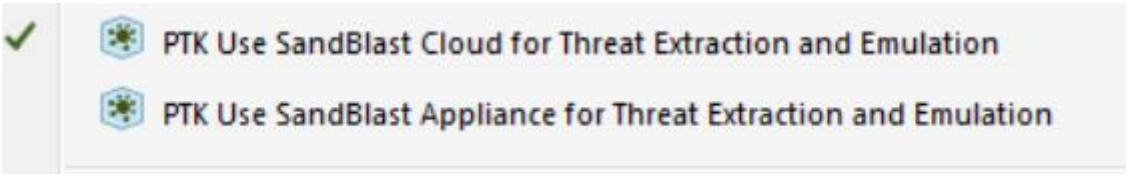


Figura 48: Configuración de la emulación en la nube en el SmartEndpoint

Figura 49: Instalando política en el SmartEndpoint

- Luego se hizo la instalación del Agente a la maquina víctima.

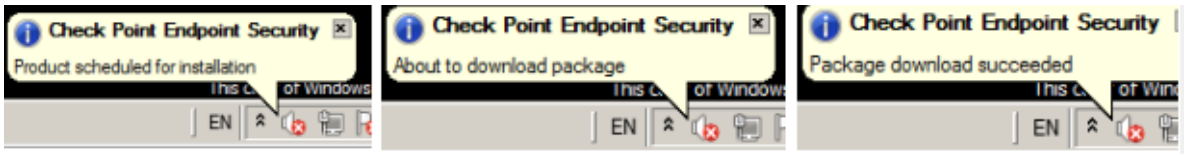


Figura 50: Despliegue de instalación del Sandblast Agent

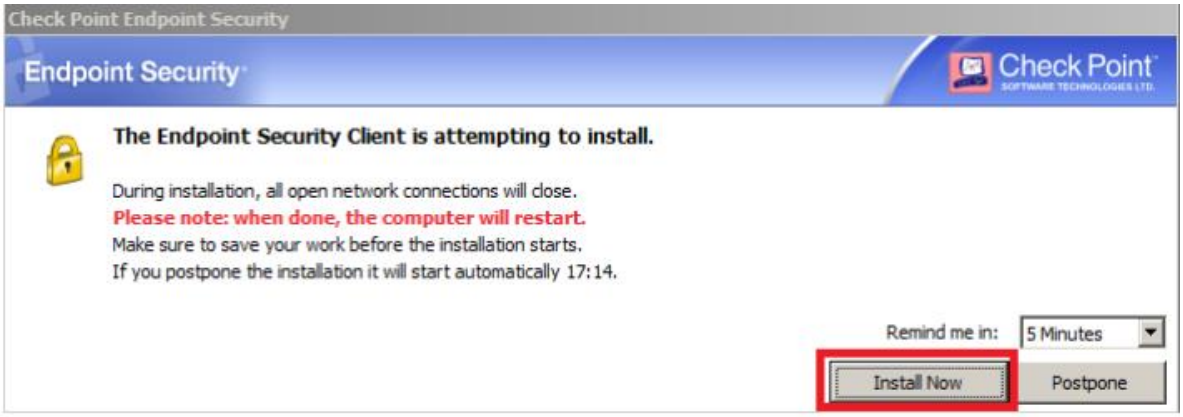


Figura 51: Instalando políticas en el Agente una vez instalado en la máquina víctima

- Luego mandamos a actualizar políticas directamente en este caso en el Agente.

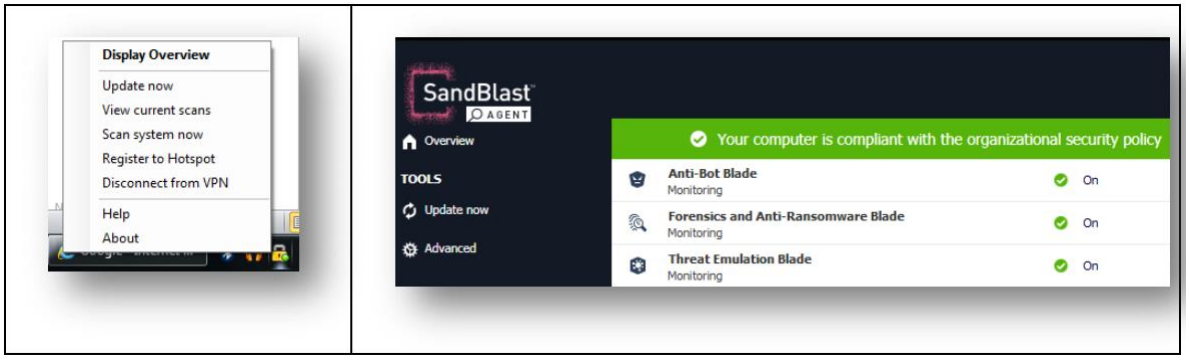


Figura 52: Sandblast Agent Instalado con blades según la política

- Luego mandamos a descargar desde el navegador de manera que se harán las emulaciones y análisis forenses.

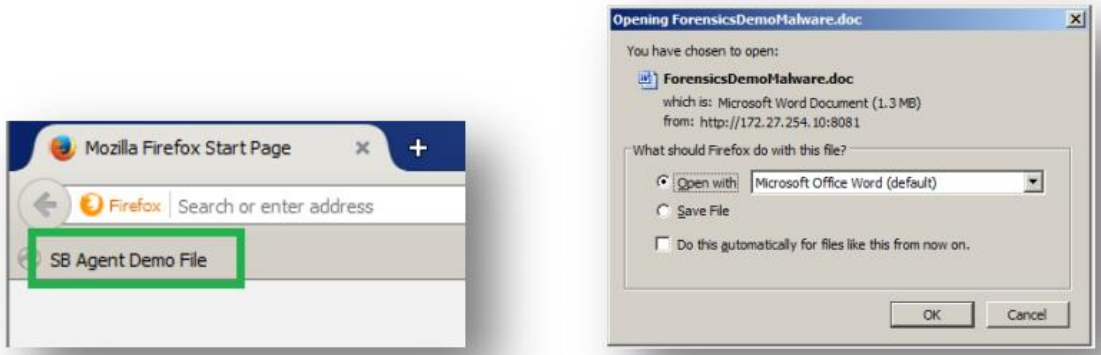


Figura 53: Descargando archivos maliciosos desde el navegador

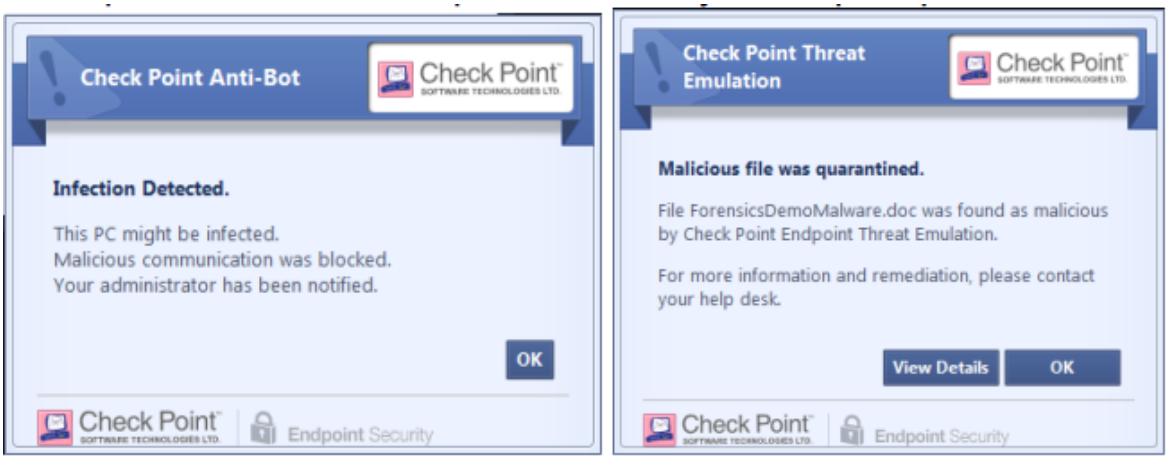


Figura 54: Detección de archivos entrantes y salientes mediante Anti-Bot y Threat emulation

- Se encontró un Botnet:

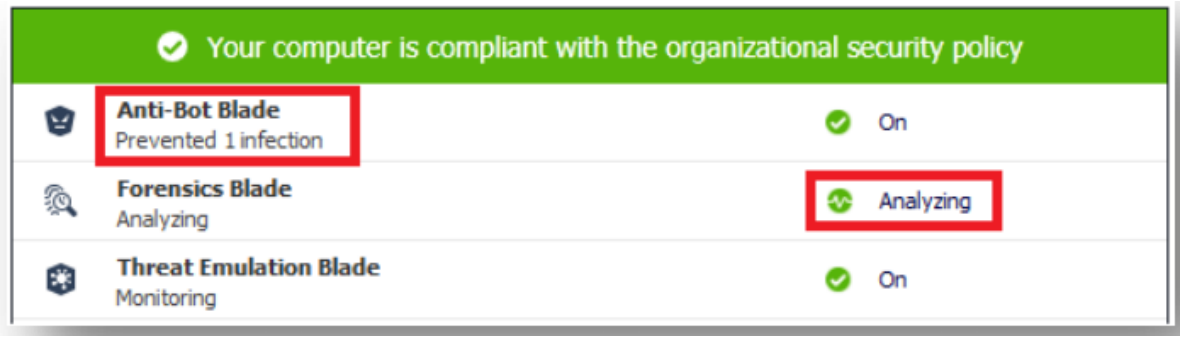


Figura 55: Análizando el incidente en el agente

Luego se hizo el análisis por medio del Sandblast Agent de cómo se propagó el Botnet.

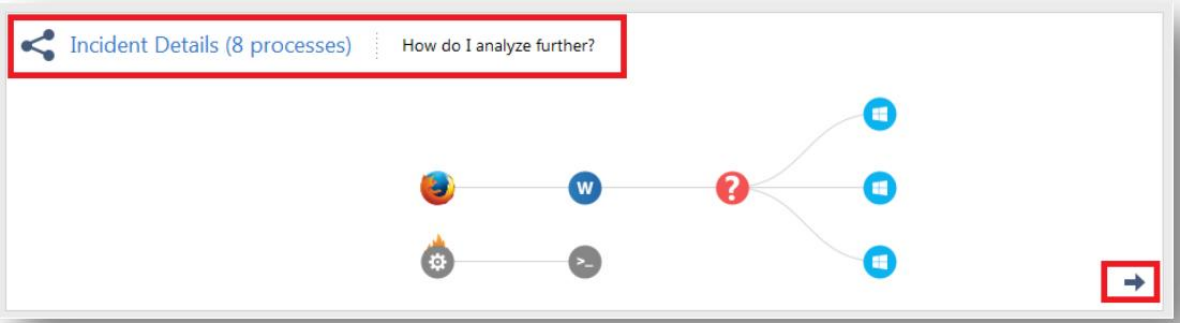
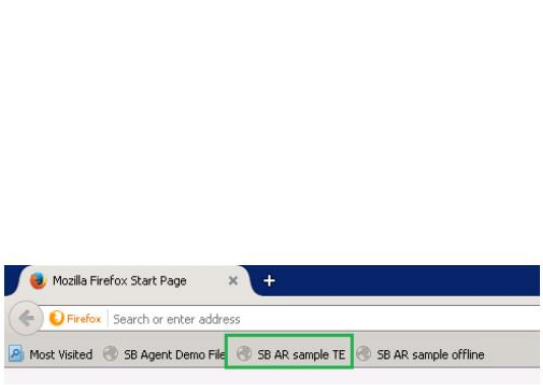


Figura 56: Detalles de los incidentes

- Se procedió a ejecutar archivos de tipo Ransomware de formato .exe



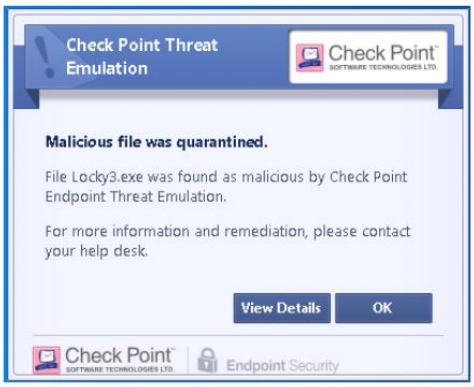
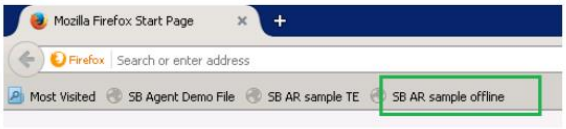


Figura 57: Descarga de archivos .exe incrustados con Malware

- Se ejecutó el script, de manera que el script desconecta al host del Check Point Threat Emulation pero el Anti-Ransomware trabaja de manera Offline también.



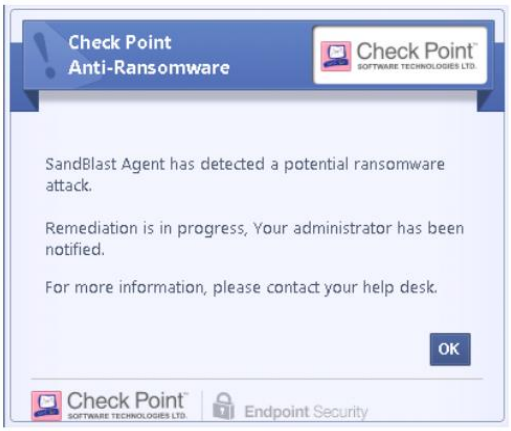


Figura 58: Descarga de Ransomware sin conexión al Threat Emulation (Offline)

4.3 Threat Extraction vía HTTP usando el Plugin de Chrome.

- Se instaló el plugins de Sandblast for Browser mediante HTTP para cualquier descarga via Web.

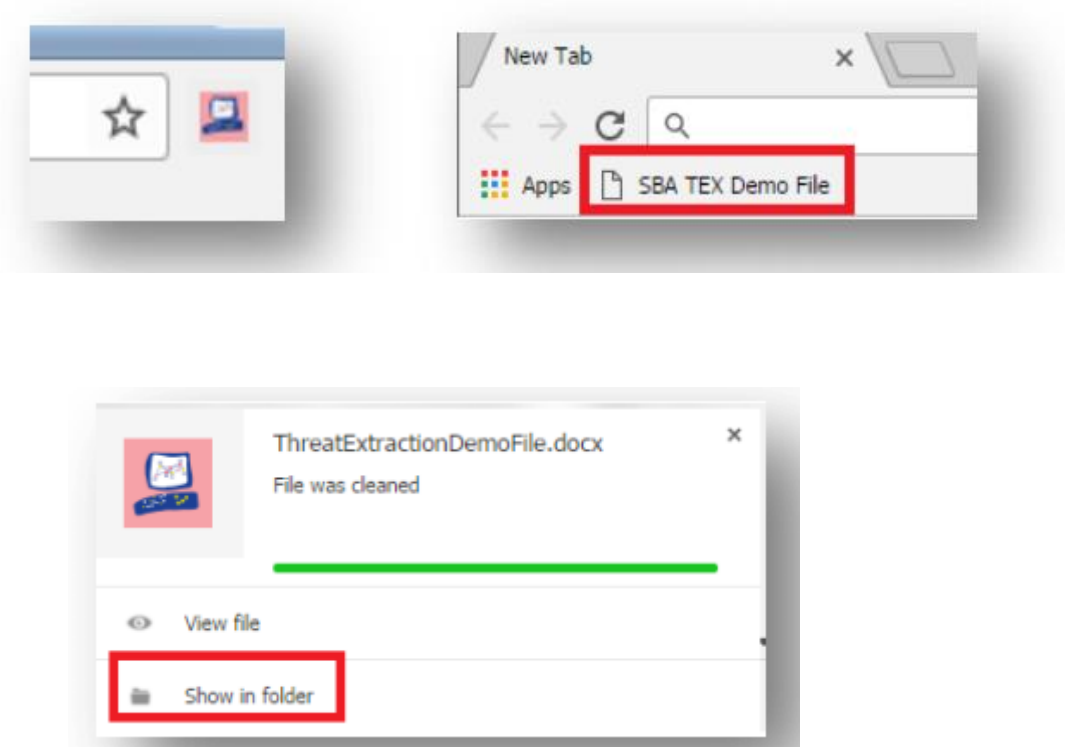


Figura 60: Archivo limpiado por Sandblast for Browser

- Donde se hizo una nueva política para la conversión a PDF en el SmartEndpoint.

Figura 61: Cambio de política en el SmartEndpoint para ser emulado vía HTTP

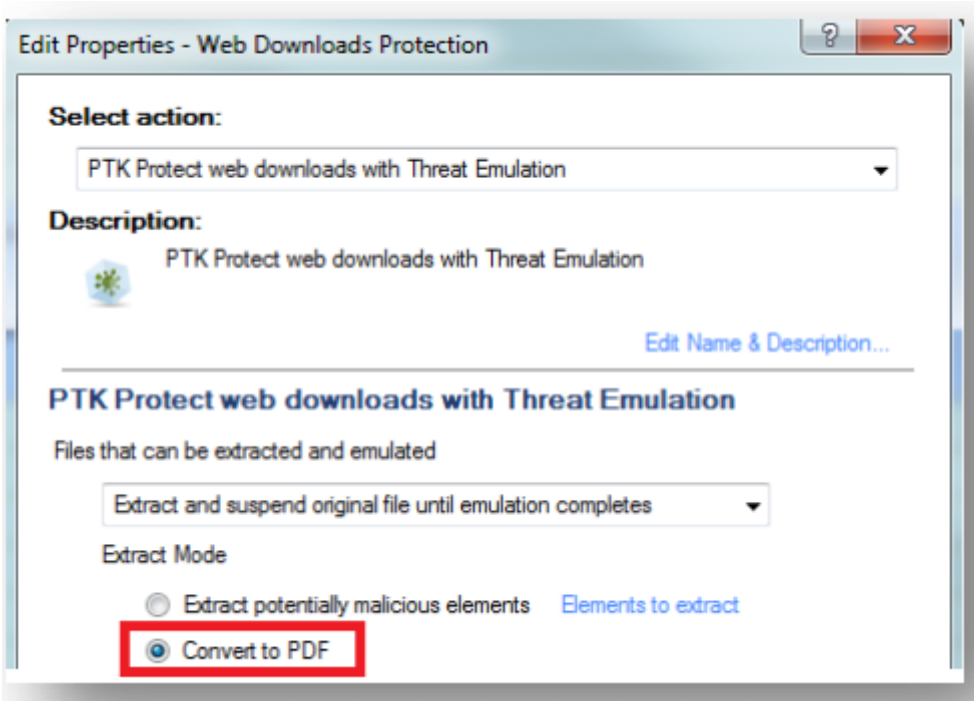


Figura 62: Cambio de política en el SmartEndpoint para la conversión a PDF

Donde cada archivo será interceptado por Sandblast for Browser vía HTTP.

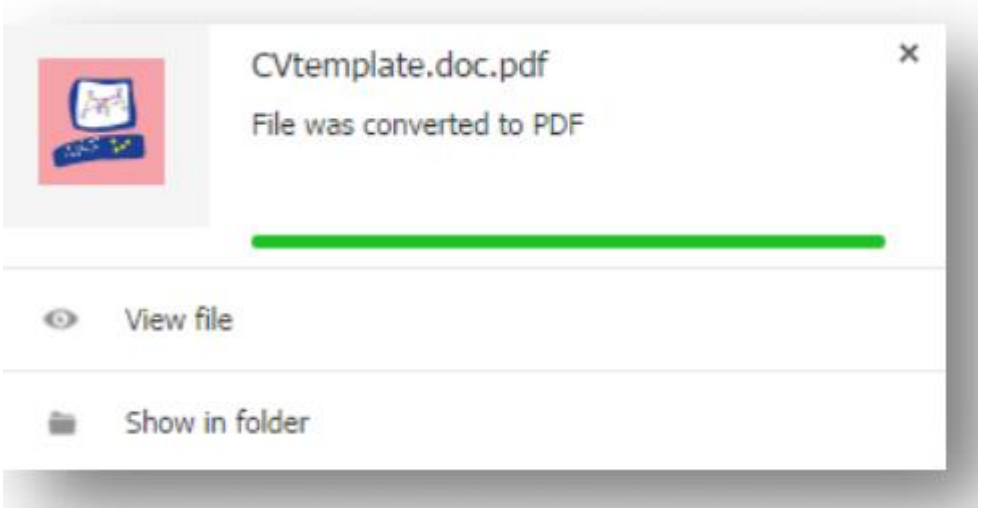
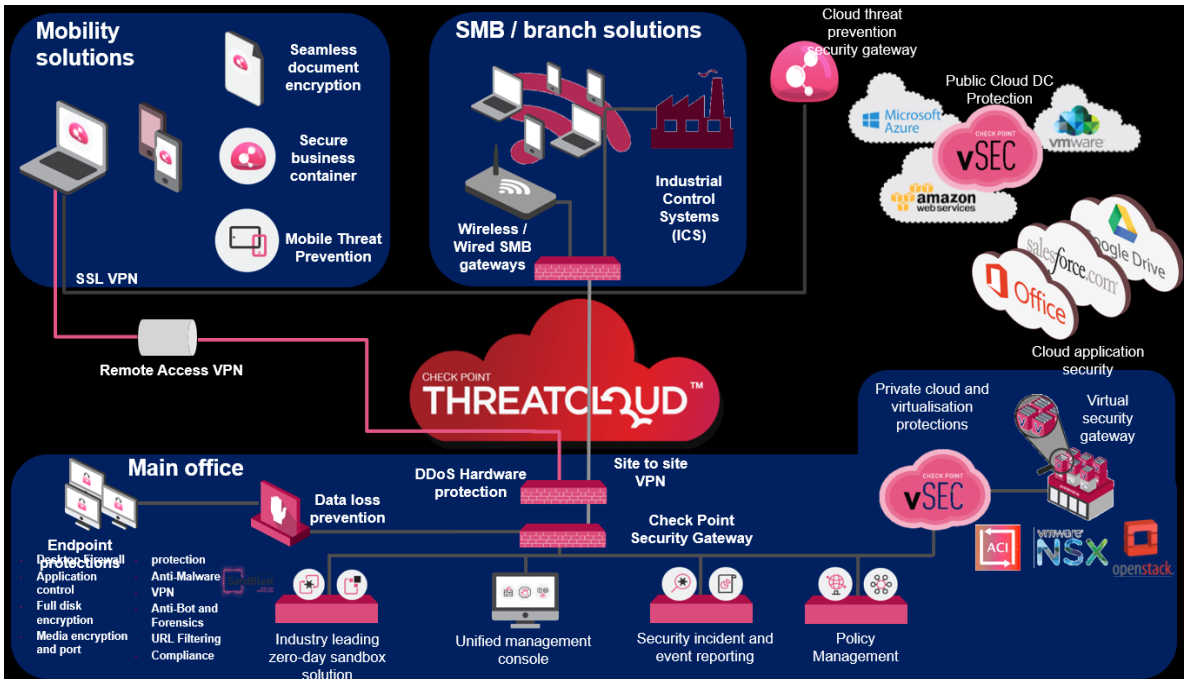


Figura 63: Descarga de archivos con malware y convertido a PDF

Estrategias de protección completa de Check Point

La compañía de Check Point recomienda una arquitectura de soluciones que deben de estar en una red informática:



Perímetro:

- DDoS Protection: Check Point ofrece un dispositivo de seguridad completa para los ataques de denegación distribuido en el perímetro.
- Gateway Network: Equipo dedicado para el perímetro con la arquitectura de Software Blades (Firewall, Application and URL Filtering, IPSec VPN, Mobile Access, Data Loss Prevention, Identity Awareness, Threat Prevention y Sandblast).

Security Management y Smart Console:

- Policy Management: Equipo dedicado para la gestión de políticas centralizados Network, Cloud y Mobile devices controlado por el Smart Console.

Correlación de eventos y reportería:

- Security incident and event reporting: Equipo dedicado para la correlación de logs y eventos en conjunto con el Security Management y así mismo los reportes.

Detección y prevención de malwares avanzados y desconocidos:

- Zero-day Sandbox: Equipo dedicado para la detección y prevención de malwares avanzados y desconocidos vía MTA (HTTP/S, SMTP/S y CIFS).

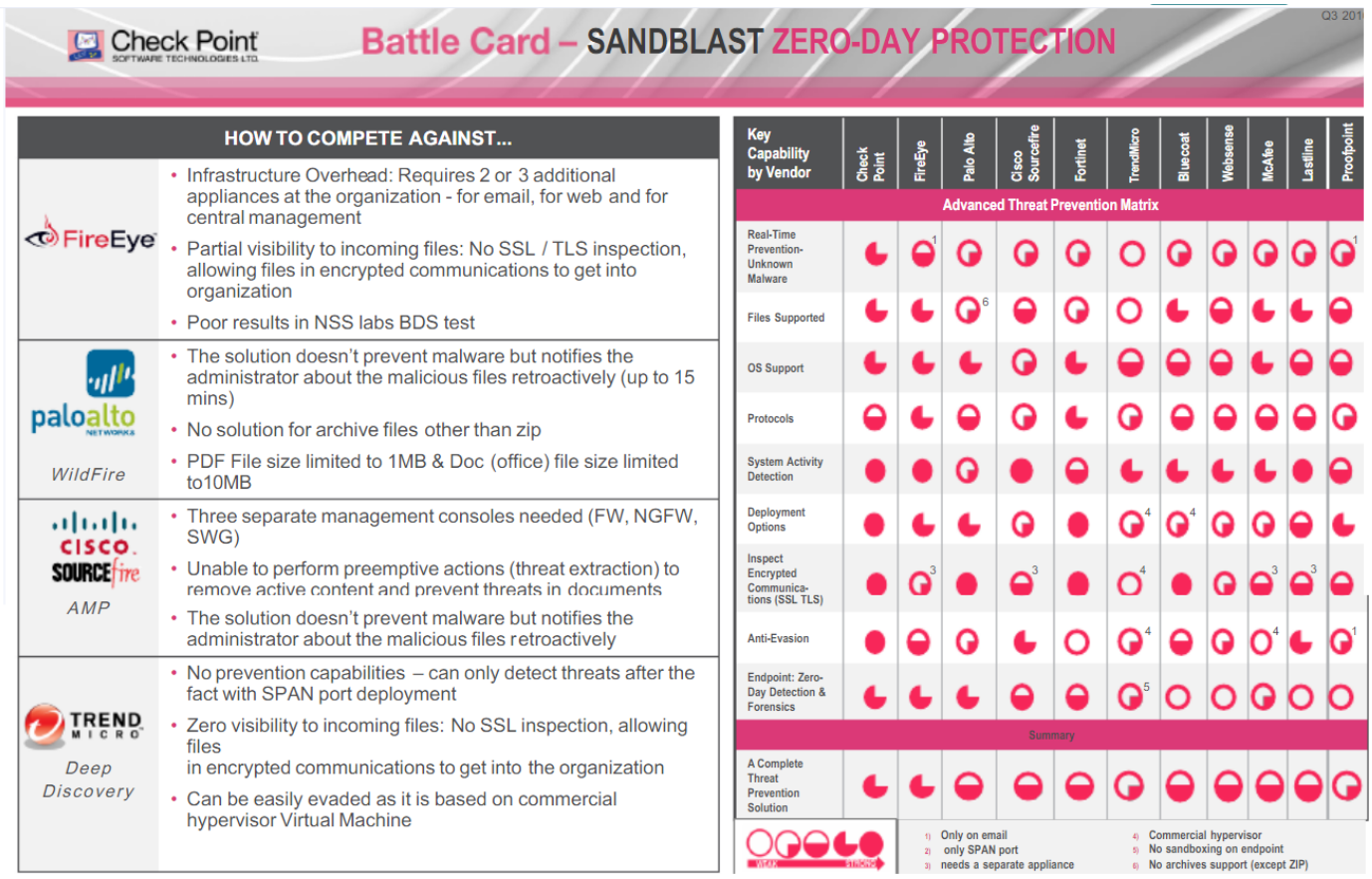
Protección para dispositivos móviles en la nube:

- Capsule: Cloud Security Gateway dedicado para equipos móviles y encriptación de archivos en los dispositivos móviles de manera segura.
- Mobile Threat Prevention: Detección y prevención de malware avanzados y desconocidos para aplicaciones móviles tanto para IOS y Android.

Protección para nubes públicas y privadas:

- vSEC nubes públicas: Software dedicado para las nubes públicas SaaS (Software como un servicio) para Microsoft Azure, Amazon Web Services, entre otros.
- vSEC nubes privadas: Software dedicado para las nubes privadas IaaS (Infraestructura como un servicio).

Tabla comparativa de la industria de Sandbox



Se tiene una tabla comparativa de todos los productos y las diferencias de las competencias de la industria de la tecnología **Sandbox** que actualmente Check Point es el más completo, entre ellos tenemos:

- Check Point.
- FireEye.
- Palo Alto.
- Cisco SourceFire.
- Fortinet (FortiSandbox).
- TrendMicro.
- Bluecoat.
- Websense.
- McAfee.
- Lastline.
- Proofpoint

Check Point vs FireEye

Check Point: La solución de Sandblast está consolidado con los Software Blades que ofrece Check Point (Firewall, Threat Prevention, Sandblast, y otros) en una sola administración, el cuál es el único **Sandboxing** más completo con respecto a detección y prevención de malware avanzados y desconocidos.

FireEye: La solución requiere de tres dispositivos (Appliances) para Web, para Correo y una para Management. El cuál no hace inspección para el tráfico cifrado via SSL/TLS.

Check Point vs TrendMicro

Check Point: La solución Sandblast ofrece una visualización y prevención completa de amenazas de tráfico cifrado (SSL/TLS) inspeccionadas en tiempo real.

TrendMicro: La solución Deep Discovery, trabaja únicamente en modo detección permitiendo todo tráfico cifrado por SSL/TLS en despliegues como SPAN Port (Puerto espejo). El cuál puede ser fácil de evadir cada máquina virtual del hipervisor.

Check Point vs Palo Alto

Check Point: La solución Sandblast previene en tiempo real malware y cada archivo .doc o .pdf tiene un análisis en tiempo de 3 a 5 minutos. También soporta muchas extensiones de archivos tales como .zip en otros.
Sandblast tiene un límite de 30 MB y como máximo 100 MB por archivos doc y pdf. Por defecto viene configurado con 20 MB.

Palo Alto: La solución WildFire no hace prevención de malware en tiempo real, pero si notifica al administrador de los archivos maliciosos como mínimo 15 minutos después. También no tiene solución a archivos de tipo .zip en otros. Documentos como PDF y DOC son limitados a 1MB y como máximo 10 MB para ser analizados únicamente.

Check Point vs Cisco SourceFire, Fortinet

Check Point: La solución ofrece una arquitectura de ciberseguridad completa de todos los Blades en un solo sistema de gestión. Además, tiene una prevención Proactiva (Threat Extraction) de la reconstrucción del archivo en limpio y removiendo malware en segundos mientras el archivo original se analiza, teniendo como opción mantener el formato original o convertirlo en PDF.

Cisco SourceFire: La solución necesita tres consolas de gestión para Firewall, Firewall de siguiente generación, SourceFire. El cuál no tiene una solución para remover contenidos maliciosos y prevención en archivos en tiempo real.

SourceFire no hace prevención de amenazas de malware, pero si notifica al administrado de dicha amenaza.

Fortinet: La solución necesita dispositivos para cada módulo y para cada tecnología. También no hace prevención de amanazas avanzadas o dirigidas.

CAPÍTULO 5 CONCLUSIONES

5.1 Conclusiones

Al culminar el trabajo de tesis concluyo que con la solución Check Point Sandblast se logra detener ataques de Ransomware Cerber, Goldeneye y Criptolocker en infraestructuras de red tanto local y entorno de usuarios finales de manera transparente tomando así una solución preventiva dinámica en un solo producto.

Con el Check Point en el perímetro se hicieron pruebas para evaluar la detección y prevención en tiempo real con análisis de eventos y forenses con funcionalidades de un Firewall de siguiente generación. El cuál protege las principales afectaciones de vulnerabilidades que pueden tener una red informática, teniendo como propuesta una arquitectura de ciberseguridad en todos los vectores dentro del mismo producto.

La tecnología Check Point ofrece planes de ciberseguridad completa para las empresas que requieren de un estricto cumplimiento de normas en el perímetro, en sucursales remotas, móviles, nubes privadas y públicas, y prevención de amenazas avanzadas. Ofreciendo mejores servicios de seguridad para todos los entornos de trabajos.

Para las empresas que combaten día a día los ataques informáticos que protegen la productividad del negocio para ello Check Point es la mejor opción en cuanto complejidad y rendimiento ante cualquier otro producto de seguridad, donde ha sido líder en la parte de Enterprise Firewall por Gartner y NSS Labs durante 20 años, y en prevención de amenazas avanzadas y desconocidas (**Sandboxing**) durante los últimos 3 años.

5.2 Recomendaciones

Instalar el equipo Check Point en el perímetro en un entorno real, donde debe tener los direccionamientos públicos y privados para así emular y extraer archivos desde el perímetro antes de hacerse la entrega correos, descargas, etc.

Estos son las topologías recomendadas para el despliegue de instalación del equipo con licencia NGTX:

Inline o SPAN Port con Check Point Gateway (NGTX) y Sandblast Appliances en premisa.

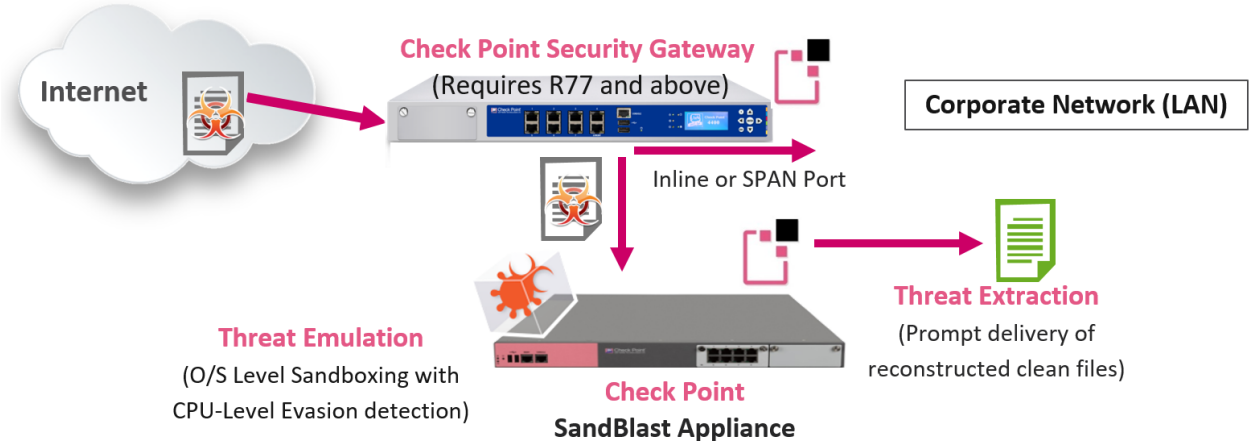


Figura 64: Despligue de instalación mediante Check Point Gateway y Sandblast Appliance con Licencia NGTX

Sandblast Appliances Standalone (NGTX)

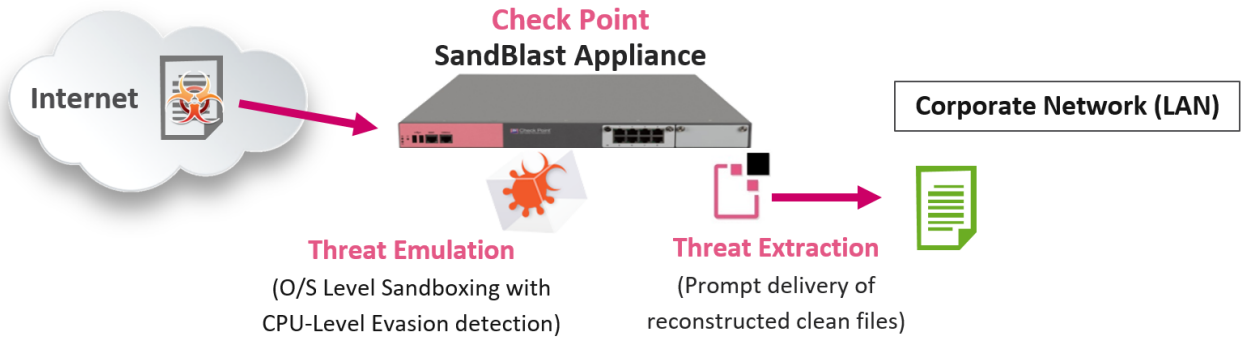


Figura 65: Despligue de instalación mediante Sandblast Appliance con Licencia NGTX (Standalone)

Inline o SPAN Port con Check Point Gateway y Sandblast Cloud Service (NGTX).

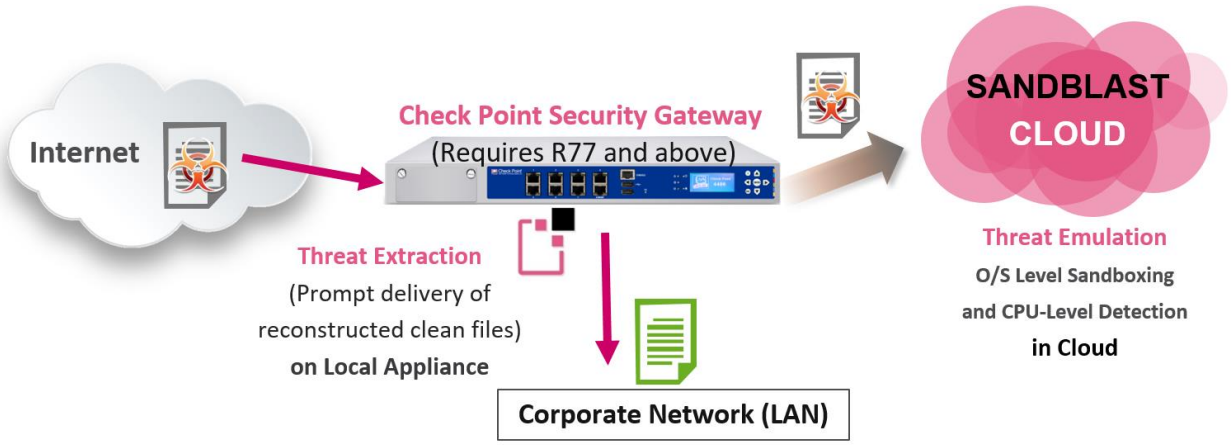


Figura 66: Despligue de instalación mediante Check Point Gateway con Licencia NGTX y emulation en la nube.

ANEXOS

5.3 Anexo 1: Domentación oficial de Check Point Sandblast Administrator.

- Check Point Software Sandblast Network and Agent

https://www.checkpoint.com/

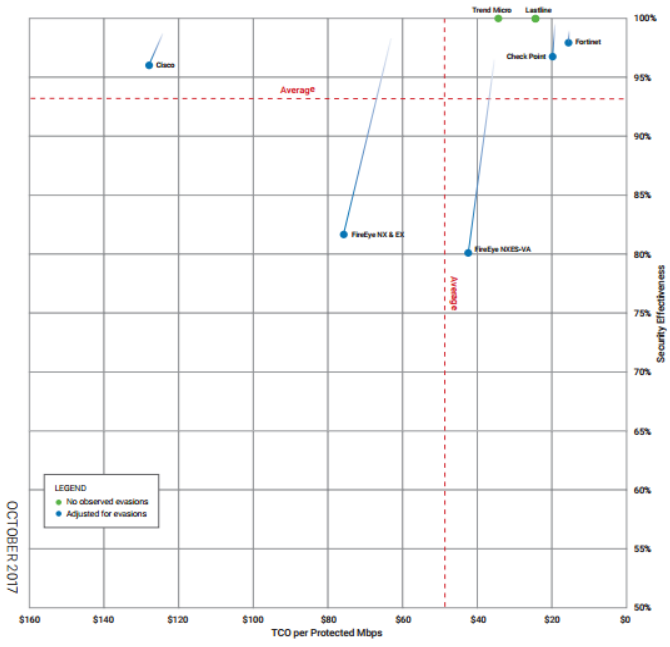
- Descarga del Check Point R77.30

https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk111841

Licencia trial por generada desde partner por 30 dias.

Enterprise Firewall 2017

Breach Detection Systems (Sandboxing) 2017



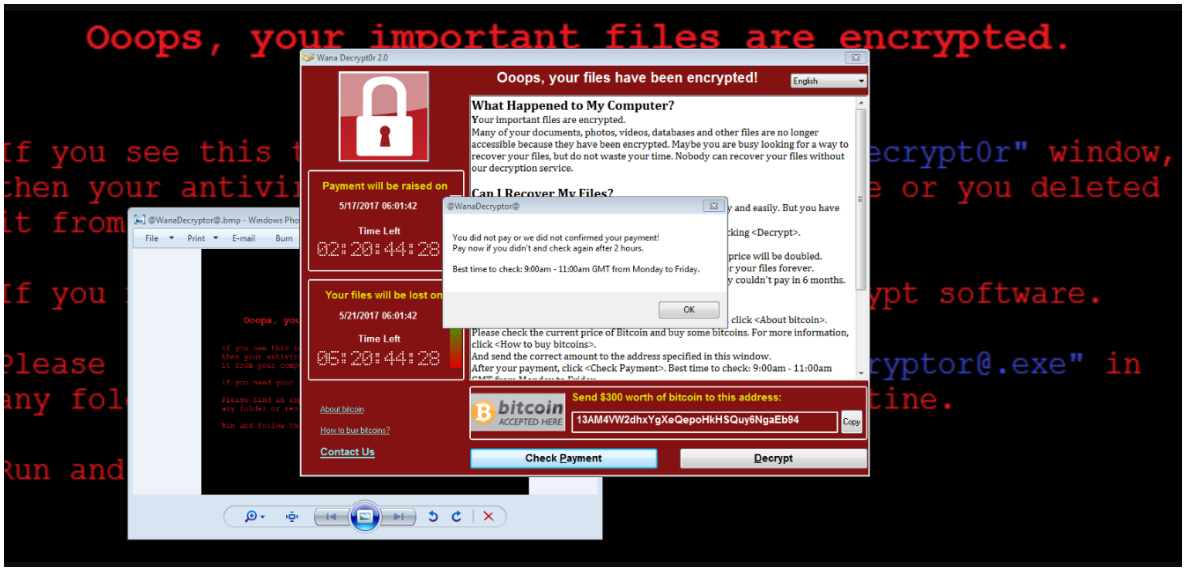
5.4 Reporte del Ransomware Wanna Cry por parte de Check Point:

Los investigadores de Check Point han estado investigando la campaña de ransomware en detalle desde que se informó por primera vez. Con un nuevo Mapa de Infección de Check Point WannaCry Ransomware, los investigadores pudieron rastrear 34,300 intentos de ataque en 97 países. El ritmo promedio a partir de hoy es un intento en cada tres segundos, lo que indica un ligero descenso desde el ritmo original registrado hace dos días, de un intento por segundo. El país más importante desde donde se registraron los intentos de ataque es India, seguido de EE. UU. Y Rusia.

Maya Horowitz, Gerente del Grupo de Inteligencia de Amenazas en Check Point, dijo: "Aunque vemos que se desacelera un poco, WannaCry aún se extiende rápidamente, apuntando a organizaciones de todo el mundo. WannaCry es una llamada de atención que muestra cuán dañino puede ser el ransomware y cuán rápido puede causar la interrupción de servicios vitales ".

El equipo de investigación e inteligencia de amenazas de Check Point anunció recientemente el registro de un nuevo dominio interruptor de muerte utilizado por una nueva muestra de WannaCry. El mapa de infecciones WannaCry Ransomware en vivo de Check Point muestra estadísticas de amenazas clave y datos específicos del país en tiempo real. El registro del dominio activó el interruptor de muerte, salvaguardando a decenas de miles de posibles víctimas contra el daño del ransomware.

Los investigadores de Check Point descubrieron que las personas afectadas por WannaCry no pueden recuperar sus archivos, incluso si pagan el rescate. Un sistema de pago y descifrado problemático y una demo falsa de la operación de descifrado pone en tela de juicio la capacidad de los desarrolladores de WannaCry para cumplir sus promesas de descifrar archivos. Hasta el momento, las tres cuentas de bitcoin asociadas con la campaña WannaCry han acumulado aproximadamente $ 77,000. A pesar de esto, ya diferencia de muchos otros tipos de ransomware, no se ha informado de un solo caso de que alguien haya recibido sus archivos.


Ooops, your important files are encrypted.
Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Payment will be raised on
5/17/2017 06:01:42
Time Left
02:20:44:28
Your files will be lost on
5/21/2017 06:01:42
Time Left
06:20:44:28
About bitcoin
How to buy bitcoins?
Contact Us
@WanaDecryptor@
You did not pay or we did not confirmed your payment!
Pay now if you didn't and check again after 2 hours.
Best time to check: 9:00am - 11:00am GMT from Monday to Friday.
OK
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Send $300 worth of bitcoin to this address:
13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94
Copy
Check Payment
Decrypt

BIBLIOGRAFÍA

(s.f). Obtenido de las configuraciones y recomendaciones de los siguientes documentos descargados desde la página de Check Point Software Blades:

- CP_R77_Gaia_Installation_and_Upgrade_Guide. Obtenido de Check Point Portal http://downloads.checkpoint.com/dc/download.htm?ID=24831

- CP_R77_Gaia_AdminGuide. Obtenido de Check Point Portal http://downloads.checkpoint.com/dc/download.htm?ID=24828

- CP_R77_Firewall_AdminGuide. Obtenido de Check Point Portal http://downloads.checkpoint.com/dc/download.htm?ID=24832

- CP_R77_SmartEvent_AdminGuide. Obtenido de Check Point Portal http://downloads.checkpoint.com/dc/download.htm?ID=24812

- CP_R77_SmartLog_AdminGuide. Obtenido de Check Point Portal http://downloads.checkpoint.com/dc/download.htm?ID=24814

- CP_R77_SmartViewTracker_AdminGuide. Obtenido de Check Point Portal http://downloads.checkpoint.com/dc/download.htm?ID=24847

- CP_R77_SecurityManagement_AdminGuide. Obtenido de Check Point Portal http://downloads.checkpoint.com/dc/download.htm?ID=24830

- CP_R77_ThreatPrevention_AdminGuide. Obtenido de Check Point Portal http://downloads.checkpoint.com/dc/download.htm?ID=24834

- CP_R77.30.03_EndpointSecurity_AdminGuide. Obtenido de Check Point Portal http://downloads.checkpoint.com/dc/download.htm?ID=53788