Universidad de Buenos Aires
Facultades de Ciencias Económicas,
Cs. Exactas y Naturales e Ingeniería
Carrera de Master en Seguridad Informática

TESIS DE MASTER EN SEGURIDAD INFORMATICA

Detección de Malware Avanzado En Redes Organizacionales y Corporativas.

Autor: Ing. Mario Ávila

Tutor: Ing. Hugo Pagola

Cohorte 2012

DECLARACION JURADA DE ORIGEN DE LOS CONTENIDOS

Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Tesis vigente y que se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual.

FIRMADO

Mario Roberto Ávila Rodriguez
DNI 94722780

AGRADECIMIENTOS

Quiero agradecer a Dios por permitirme llegar donde estoy, a mi padre Roberto Ávila por enseñarme siempre ser una persona íntegra en valores, a mi madre Evamaría Rodríguez que me ha enseñado a ser persistente en mis metas y objetivos, al director de tesis y a las personas cercanas que me han apoyado para que el desarrollo de este proyecto salga adelante.

To Sandy Cheeks, Mataderos, Buenos Aires Septiembre 2014.

TABLA DE CONTENIDO

INDICE DE FIGURAS

INDICE DE GRAFICAS

INDICE DE TABLAS

1. INTRODUCCION

Actualmente los mecanismos utilizados para la evasión y transmisión de código malicioso por parte de los desarrolladores de malware han cambiado en la última década. Ante el dinamismo en el cambio de las redes, se crean nuevas metodologías para evitar la seguridad utilizando conceptos como amenazas día Zero o algoritmos ***DGAs***, donde nuevos métodos avanzados han sido desarrollados para eludir la detección de malware siendo esto uno de los principales problemas para las tecnologías de seguridad de primera generación existentes como los antivirus, firewalls, antispams, etc.

Una de las principales preocupaciones es que este tipo de malware puede infiltrarse en redes de gran escala sin ser detectado por las tecnologías de seguridad actuales durante largos periodos. Por ello, a pesar de los nuevos conceptos de seguridad como ***sandboxing*** que evitan el daño que puede producir el malware en los ambientes de producción, ya se conocen técnicas y ataques avanzados como el caso del malware ***FLAME*** [1]. Este malware durante los ciclos del ataque pudo eludir la detección a pesar de la seguridad actual que existía en su objetivo siendo uno de los mayores casos de estudio de malware que realizaron múltiples fabricantes.

Debido a esto y ante la preocupación de los nuevos métodos desarrollados por el negocio organizado de los atacantes y grupos hacktivistas, los fabricantes de tecnología de seguridad han diseñado soluciones catalogadas como ***técnicas y tecnología de próxima generación*** para la detección y control dinámico de las amenazas actuales en las organizaciones.

En esta investigación se trabajó en estudiar, detectar y comprender a nivel de red el comportamiento antes las múltiples amenazas y técnicas utilizadas por el malware avanzado en las redes corporativas. Se utilizaron tecnologías de seguridad de próxima generación para el análisis del malware, también se realizaron

encuestas y se estudiaron topologías reales en el mercado para obtener un relevamiento de información de las arquitecturas típicas de las redes corporativas, financieras, gubernamentales, etc. Se implementó un caso práctico en el cual se analizó como utilizar las tecnologías estudiadas para reforzar la seguridad existente y de esa forma contrarrestar los ataques de los malwares seleccionados. Las pruebas se realizaron sobre un laboratorio controlado aislado utilizando la plataforma de virtualización VMware que permite simular máquinas, servicios y también implementar dispositivos virtualizados de detección de malware dentro de la topología estudiada y seleccionada.

En la arquitectura implementada, se infectaron maquinas con muestras de malware conocidos mundialmente para realizar pruebas, análisis y visibilidad de todo el contexto y estado de la red. En base a los resultados de estas pruebas, se pudo analizar y determinar el comportamiento de diferentes técnicas de malware y confeccionar una guía para la implementación adecuada de un sistema de próxima generación que ayude a reforzar las redes actuales ante las nuevas amenazas, vectores de ataques y técnicas emergentes utilizadas por el malware avanzado.

1.1 PALABRAS CLAVES

- **Malware:** Software malicioso o dañino que realiza funciones no deseadas o anomalías alterando los programas y la información dentro de un computador u ordenador afectando su funcionamiento normal.

- **Sandboxing**: Técnica utilizada para aislar un programa no conocido de manera separada en un ambiente controlado De esta forma se ejecuta el programa de manera controlada y si algún error o incidente de seguridad ocurre debido a la ejecución del programa gracias a su aislamiento este no afecte al ambiente y sectores donde se ejecutan los demás programas.

- **Tecnología de primera generación:** Las tecnologías de primera generación se denominan a las primeras soluciones de seguridad de datos, plataformas de red, dispositivos, servidores y maquinas finales por Ej.: Router ACLs, Firewall, IPS, VPN, Antivirus, NAC, etc.

- **Tecnología de próxima generación:** Tecnología desarrollada con el fin de complementar la seguridad que no es abarcada a nivel de capas por la tecnología de primera generación. Un ejemplo puede ser un ***Next Generation IPS*** el cual estudia el contexto de una red (dispositivos, servicios, aplicaciones, vulnerabilidades, etc) y basado en esta información brinda de manera automática recomendaciones para la activación de reglas, reforzando así la seguridad de la red, dispositivos y maquinas servidores/clientes.

- **DGA:** Algoritmo de Generación de Dominios utilizado por creadores de malware con el fin de generar de manera automática una lista de sitios aleatorios y no válidos. De esta forma el malware desde la máquina infectada, trata de conectarse a estos dominios con el fin de establecer comunicación con el sitio valido que apunta al atacante y se encuentra escondido dentro de la lista. Una vez se establece la conexión desde la maquina infectada, el malware puede recibir nuevos comandos, instrucciones y actualizaciones por parte del atacante [2].

- **Spear phising:** Utiliza el concepto de ingeniería social para conocer información de las casillas de correo de los usuarios en la empresa. Posteriormente mediante un mail enviado a estos, el atacante simula ser un sitio de confianza financiero o comercial conocido en la web para tratar de persuadir a los usuarios a que ingresen información sensible o confidencial de la organización. Por lo general también utilizan links dentro del mismo correo para enrutar a sitios catalogados con contenido de malware.

- **Amenaza día Zero:** Es un tipo de ataque que explota una vulnerabilidad totalmente desconocida aún por los desarrolladores de una aplicación o sistema operativo. Potencialmente es utilizada por los desarrolladores de malware para realizar ataques mediante *exploit kits* y crear nuevos vectores de ataques.

- **Hypervisor:** Software o hardware base diseñado para crear y correr máquinas virtuales dentro de una plataforma tecnológica. Inicialmente Hypervisor fue un sistema operativo diseñado para la división de múltiples tareas de procesamiento en un servidor que cuenta con recursos físicos disponibles.

- **CVE:** Common Vulnerabilities and Exposures. Es un listado de estándares relacionados con las amenazas de seguridad existentes para diferentes sistemas operativos y aplicaciones. Estas amenazas se listan a través de dos categorías como vulnerabilidades y exposiciones. Una vulnerabilidad está asociada al ámbito de computadora, servidor o red que presenta en definitiva un identificable riesgo de seguridad en un contexto. Una exposición está asociada a una situación relacionada con la seguridad, evento o acto, que puede ser también considerado una vulnerabilidad por algunos pero no por otros.

- **CnC: *Command and Control***: Pueden ser conexiones seguras o no seguras originadas directamente por botnets o maquinas infectadas con malware desde redes internas hacia servidores o dominios externos. Su objetivo principal es permitir a la maquina infectada o bot recibir nuevos comandos de acción, actualizaciones de códigos y mensajes de instrucciones desde el servidor atacante.

- **Blended threats:** Son exploits que combinan diferentes módulos de malware existentes en el código para posteriormente ser utilizados y emplear múltiples vectores de ataque. Incrementan la severidad del daño en los sistemas a través de múltiples infecciones, técnicas de ocultamiento y velocidad de contagio. Actualmente existen diversos malwares conocidos con estas propiedades como *CodeRed, Bugbear, Conficker* entre otros. Por lo general son detectados como virus, gusanos o troyanos hoy en día.

- **Antispam:** Soluciones de software o hardware basadas en el análisis de protocolos de correo SMTP y POP3. Utilizan técnicas de monitoreo de reputación del origen de sitios y contenido malicioso dentro de los mensajes de correo logrando filtrar correo *Spam* (basura), Antisphing, etc. Este tipo de herramientas pueden realizar un análisis a nivel heurístico para detectar dentro de los archivos adjuntos malware o archivos sospechosos utilizando técnicas de cuarentena o limpieza de archivos.

- **Malware Cloud Lookup:** Análisis en la nube que realizan tecnologías de próxima generación para la consulta del estado de archivos que son transmitidos a través de protocolos de aplicación como FTP, HTTP, HTTPS, entre otros. Inicialmente se transmite el resultado de una función hash tomada directamente del archivo y luego es enviado a la nube donde se encuentran los laboratorios de detección para nuevas amenazas y casos conocidos de malware. Posteriormente esta información es enviada al software de seguridad para que ejecute cierta acción dependiendo el resultado de riesgo de la consulta.

- **BYOD: Bring Your Own Device** Concepto adoptado por las empresas para permitir que sus empleados o usuarios puedan conectar sus dispositivos móviles (laptops, tables, smartphones, etc) a la infraestructura tecnológica. De tal forma que puedan acceder a los servicios y activos de información de

la organización, los dispositivos son administrados desde una consola central que facilita el monitoreo y controla los accesos a datos y aplicaciones de la empresa.

- **SIEM: Security *Information and Event Management*** Software que recolecta, resguarda y correlaciona todos los eventos y alertas de manera centralizada de los dispositivos de hardware y aplicaciones de software en una infraestructura tecnológica. También permite recolectar logs y paquetes asociados de eventos para realizar un análisis a tiempo real de la información. Las herramientas SIEM evolucionaron a nivel de seguridad para poder visualizar el flujo de la información recolectada, creando reportes específicos para las regulaciones y normas de cumplimiento que recaen en las organizaciones**.**

- **VDI: *Virtual Desktop Infraestructure*** Tipo de infraestructura tecnologica que brinda servicios centralizados de conexión remota a los usuarios de red. Levanta y conecta una sesión virtual de escritorio independiente para cada usuario utilizando protocolos RDP o ICA, de esta forma ofrece servicios de desktops sin necesidad de maquinas fisicas o de escritorio.

  Los usuarios se pueden conectar desde cualquier red que alcance a servidor VDI principal y acceder a la sesion de desktop asignada sin necesidad de estar atados a un cliente fisico. Gracias a la centralizacion de escritorio de usuarios estos también acceden a aplicaciones y datos. Este tipo de infraestructuras permite a los administradores de IT soportar de manera mas eficiente y centralizada los incidentes en las organizaciones.

- **MDM: *Mobile Device Management*** Herramienta administrativa centralizada que permite implementar, asegurar, monitorear e integrar los dispositivos móviles como smartphones, tablets y laptops al área de trabajo, sin comprometer la seguridad de las aplicaciones y datos de la organización.

2 OBJETIVOS

2.1 OBJETIVO GENERAL

- Detectar y analizar tráfico de malware avanzado en redes organizacionales y corporativas.

2.2 OBJETIVOS ESPECÍFICOS

- Estudiar el contexto tecnológico de redes organizacionales y corporativas actuales que cuentan con arquitecturas de seguridad de primera generación.

- Implementar utilizando tecnología de virtualización VMWARE una red de prueba para simulación de ataques y técnicas de malware avanzado.

- Analizar y detectar en el espectro del tiempo (antes, durante y después) ataques de malware avanzado utilizando tecnología de próxima generación.

- Diseñar guía o metodología que brinde mejores prácticas para la implementación de tecnología de próxima generación que trabaje de manera complementaria con la seguridad de redes típicas organizacionales y corporativas actuales para la protección ante ataques y técnicas de malware avanzado.

3 ALCANCES Y LIMITACIONES

3.1 ALCANCES

- Realizar encuestas a un número representativo de administradores, consultores y técnicos de tecnologías de seguridad e infraestructura tecnológica actual para conocer las arquitecturas y servicios críticos dentro de las organizaciones.

- Analizar arquitecturas típicas de servicio y seguridad actual de grandes redes de datos corporativas, financieras, gubernamentales, tanto ambientes con tecnología física como virtual etc a partir de casos de uso conocidos.

- Cubrir las necesidades del cliente en base a las características de su organización utilizando tecnología de detección de contexto de ambiente.

- Implementar red con servicios a escala con seguridad de primera generación utilizando tecnología de Virtualización VMWARE.

- Reforzar a través de tecnología de próxima generación la red simulada.

- Detectar y controlar utilizando tecnologías de próxima generación técnicas utilizadas por el malware avanzado en la PoC.

- Realizar conclusiones y documentación de resultado de las pruebas de la PoC

.

- Todo el laboratorio se realizará sobre plataforma virtual. Se establecerán los límites de las tecnologías a utilizar en el laboratorio debido a los recursos virtuales disponibles para la PoC.

3.2 LIMITACIONES

- Las técnicas para la simulación se basarán en muestras de malware conocidas actualmente para las plataformas a nivel de red.
- Las plataformas utilizadas para la PoC son sistemas operativos y servicios basados en los resultados del estudio de topologías.
- No se realizaran estudios intrínsecos de malware en las maquinas finales, servidores o servicios.
- Se presentará solución de próxima generación basadas bajo el concepto de Agile Security.
- La guía de implementación de tecnología de próxima generación se limitará a los resultados de las investigaciones y arrojados de la prueba de concepto.
- Las maquinas finales, servidores y sus servicios no contaran con soluciones de seguridad locales o a nivel de endpoint debido a que se está tratando de simular y estudiar el comportamiento de malware a nivel de red, no localmente.
- Las tecnologías en plataformas de virtualización, seguridad y networking a utilizar son OpenSource y Comerciales, solo se cuenta con licencias demostrativas o de prueba solamente para utilizar sus funciones de manera investigativa, no son plataformas licenciadas completamente, las cuales son:

- **WMARE ESX:** Tecnología para la virtualización de plataformas y aplicaciones de la red a simular.

- **Microsoft Windows:** Tecnología para la implementación de servidores, clientes y servicios de networking entre otros.

- **SNORT:** Tecnología OpenSource para análisis de forma intrusiva del tráfico de red.

- **Checkpoint:** Marca especialista en soluciones de seguridad con varios productos en el mercado para ambientes de redes y datos organizacionales.

- **KerioConnect:** Software que permite la implementación de servicios y casillas de correo para el envío y recepción a través del protocolo SMTP

- **Microsoft SQL Server 2008 Express:** Tecnología que permite implementar servicios de base de datos a través de instancias locales creadas bajo un sistema operativo.

4 MARCO TEORICO

4.1 RESEÑA SOBRE STUXNET

En junio del 2010, ***Kaspersky Lab*** comenzó un análisis heurístico de los que sería una de sus mayores anomalías conocidas a nivel de malware. Todo inicio mediante una llamada por parte de uno de sus principales clientes, donde al principio informaba que existían maquinas dentro de la organización las cuales se booteaban constantemente de manera automática y sin razón alguna entendible.

Al inicio, este comportamiento fue asociado a un virus conocido por parte de los ingenieros que afectaba directamente el sistema de booteo de las plataformas Windows. A medida que analizaban el código fuente (utilizando técnicas como ingeniera inversa) pudieron encontrar comportamientos relacionados con técnicas avanzadas que trabajaban de manera conjunta y jamás vistas dentro del código malware. También detectaron ciertos patrones avanzados de propagación y ocultamiento utilizados por métodos totalmente desconocidos de scripting, siendo indetectables por los motores de antivirus en ese momento.

Desde entonces ante la luz de todo lo descubierto, los ingenieros de Kaspersky junto con la colaboración de comunidades y otros fabricantes de seguridad se encontraron ante el primer caso de malware avanzado en el mundo donde más tarde fue conocido y nombrado como ***Stuxnet.*** Según el análisis, su objetivo primordial y por el cual fue diseñado era alterar o sabotear el funcionamiento de los PLC que controlaban los reactores de uranio, los cuales eran manipulados por equipos que trabajaban bajo el sistema operativo Windows.

Los ataques fueron basados en vulnerabilidades día zero desconocidas por el fabricante en su momento. Esto extrañó inmediatamente a los ingenieros ya que evidenciaron nuevos métodos de comunicación por parte de malware al notar que

trataba de iniciar una conexión interna hacia servidores externos. Este tipo de conexiones permitían brindarle información al atacante sobre el estado actual de las plataformas, más adelante, los investigadores concluyeron que el malware fue diseñado de tal forma que ayudara a alterar específicamente lo sistemas de control de Siemens, encargados de manipular las centrifugadoras de Uranio en el programa nuclear Iraní.

Las conclusiones referentes al análisis de Stuxnet conllevaron a que su algoritmo complejo indicaba que los atacantes diseñaron técnicas avanzadas de propagación y no detección a diferencia de otros malwares hoy en día. Los investigadores también afirmaron que este tipo de ataques fueron construidos directamente por entidades u organizaciones que financiaron el desarrollo debido al tiempo e inversión que demandaba el código para lograr las funciones avanzadas detectadas. Al final, concluyeron que Stuxnet fue creado para sabotear las máquinas controladoras de uranio iraní y su desarrollo directamente fue soportado por el gobierno de Estados Unidos debido al conflicto y la controversia del plan de enriquecimiento de uranio realizado por Irán.

En la figura 1 se puede ver los diferentes tipos de malware avanzados conocidos y como crece su complejidad basada en las técnicas utilizadas por su predecesor. A continuación se estudia el malware Flame y su relación directa con el análisis realizado sobre el malware Stuxnet [4].

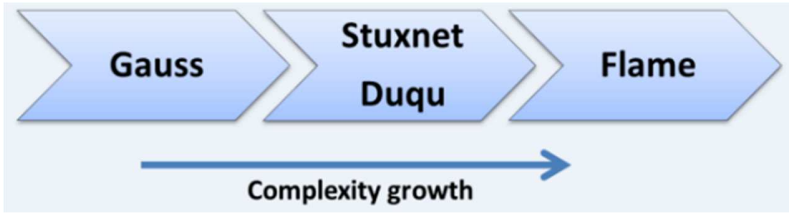


Figura 1. Evolución complejidad del malware [14]

4.2 RESEÑA SOBRE FLAME

A finales del año 2012, otro caso de malware avanzado fue reportado ante Kaspersky donde inicialmente los ingenieros apuntaron a una nueva variante del malware *Stuxnet*, en este caso encontraron nuevas técnicas relacionadas al ciberespionaje que nunca habían sido vistas en código anteriores. Haciendo referencia a la investigación realizada por el laboratorio de criptografía y seguridad en sistemas *CrySys* este nuevo malware tenía los mismos comportamientos de propagación que *Stuxnet* pero además podía enviar información mucho más compleja y detallada de la organización mediante mensajes no estructurados como imágenes, mensajes de chats e incluso poder grabar conversaciones utilizando dispositivos de grabación lógica y física.

Otros métodos avanzados fueron detectados en el código para la propagación, utilizando técnicas de gusano a través de conexiones vía Bluetooth que son activadas por los pacientes cero del malware para infectar máquinas dentro del alcance al rango de la señal. No solamente este tipo de comportamiento alertó a los investigadores sobre esta nueva amenaza, sino que también el tamaño del archivo completo utilizado por el malware era aproximadamente 20MB (40 veces más del tamaño del Stuxnet) el cual contenía módulos internos utilizados netamente para sus funciones avanzadas de propagación, infección, ocultamiento, entre otras[1].

Flame como fue mundialmente conocido después este malware a diferencia de su predecesor Stuxnet, no buscaba realizar un ataque directo en los sistemas sino que a través de técnicas avanzadas de ocultamiento, manejaba rutinas de interrupción que le permitían esconder y ser indetectable en infraestructuras no convencionales para evitar ser detectado por tecnologías de seguridad. De esta forma buscaba poder adentrarse dentro de las plataformas durante largo tiempo

[1] Información tomada del reporte técnico de Skywiper a complex malware for targeted attacks., *Laboratory of Cryptography and System Security (CrySyS)*

para obtener mayor información sobre la infraestructura y seguridad de las organizaciones víctimas.

Flame ha sido catalogado como uno de los malware más completos y complejos hoy en día ya que su arquitectura permite utilizar patrones conocidos de actualización automática en los sistemas operativos como Windows Update. También puede crear certificados falsos y una ingeniería casi perfecta e ingeniosa utilizando el paciente cero como servidor principal para la propagación del malware a través de los procesos WSUS.

Hasta el momento se conocen dentro de las variantes de Flame hasta 15 módulos los cuales ejercen diferentes funciones dentro del malware para asegurar el ataque.

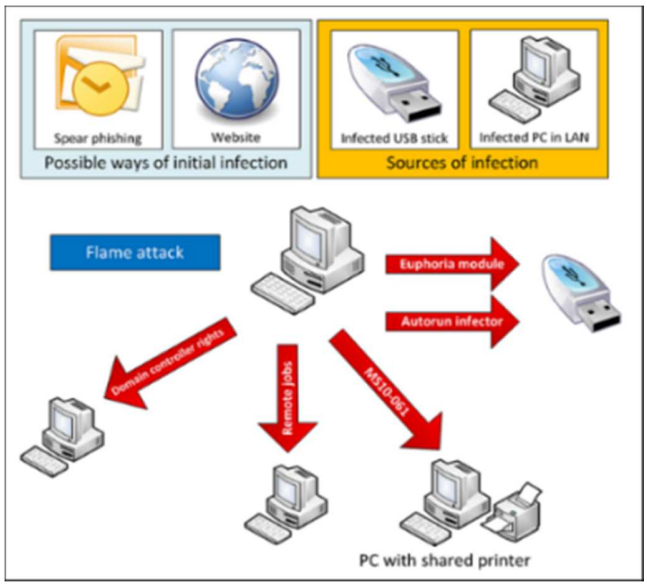


Figura 2. Métodos de propagación Flame [15]

Conociendo un poco más sobre las variantes de malware avanzado existentes, el estudio principal y objetivo de esta investigación fue conocer el tipo de técnicas empleadas por parte del código malicioso avanzado Stuxnet o Flame, así ayuden a poder visualizar la infección, detección y propagación del malware dentro

del tráfico normal en las comunicaciones de grandes redes organizacionales y corporativas.

4.3 EVOLUCION DE LAS AMENAZAS TIPO “BLENDED THREATS”

Los ataques de malware hoy se conocen como amenazas tipo ***blended threats*** ya que utilizan técnicas conjuntas las cuales combinan diferentes métodos utilizados por virus, gusanos, troyanos, backdoors, etc. Las tecnologías de seguridad tratan de ir a la vanguardia de los avances en el desarrollo de malware, no obstante lo que realmente preocupa y alerta a la comunidad de seguridad actual es que el malware ha dejado de ser utilizado solamente simplemente para fines delictivo, sabotaje o robo de información propietaria por ejemplo sino que a través de técnicas persistentes avanzadas buscan perpetuar ataques puntuales logrando robar información sobre la topología e infraestructuras tecnológicas en las organizaciones.

Una vez las redes están comprometidas, el malware puede enviar información de casi toda una topología de servicios y dispositivos a los atacantes ya sea de manera automática o los atacantes accedan a las máquinas para obtener acceso a los sistemas a través de privilegio, con el control comprometido de las máquinas, servidores u dispositivos pueden modificar o alterar plataformas completamente operativas, robando información altamente sensible o logrando incluso volver al malware indetectable por los sistemas de seguridad. Uno de los casos más comunes sobre amenazas persistentes fue el caso Stuxnet en particular [5].

El concepto y la forma de brindar de seguridad ante un nuevo ataque de malware en los últimos 5 años ha cambiado considerablemente, las herramientas de seguridad se deben adaptar al contexto que existen en la red para lograr conocer y proteger la mayor parte posible de los sistemas ante la eventualidad de un incidente de seguridad. Por ello, las tecnologías mayormente desarrolladas y sean opensource o comerciales buscan de manera preventiva conocer en lo posible el comportamiento de los ataques realizados dentro de las infraestructuras.

A esto se suma que la complejidad de las redes aumenta a nivel de infraestructura, donde los nuevos tipos de servicios son brindados utilizando como base plataformas virtuales que trabajan bajo tecnologías como Hypervisor. Si bien hace más de treinta años la virtualización comenzó a trabajar en los sistemas de IBM (comúnmente conocidos como ***MainFrame)*** en la actualidad desde hace más de 10 años este concepto ha sido reforzado y llevado en las grandes organizaciones, por lo que un sin número de servicios hoy en día son implementados gracias al poder de la virtualización.

En paralelo, cabe destacar que esto a su vez ha ayudado a los desarrolladores de seguridad a manejar nuevos conceptos y a desarrollar técnicas más avanzadas como ***sandboxing*** e inclusive utilizar ambientes virtualizados para el estudio a fondo de malware y sus ataques. Esto más adelante conllevo a hablar sobre un nuevo concepto en la actualidad a nivel seguridad como lo son las tecnologías de próxima generación, que utilizan este tipo de conceptos y análisis continúo para las nuevas amenazas.

4.4 EVOLUCION TECNOLOGIAS DE PRIMERA GENERACION

A principios del 1994, el fabricante de tecnología ***Checkpoint Software*** introdujo el concepto de Statefull Firewall dentro de sus soluciones de seguridad a nivel de Firewall siendo uno de los primeros también en introducir el concepto de tecnología de próxima generación en las redes. Si bien a finales de los noventa aún se utilizaban técnicas avanzadas en los malwares, solo hasta comienzos del 2008 (casi 11 años más tarde) se conocieron los primeros ataques de seguridad sobre plataformas Windows que apuntaban directamente a realizar acciones precisas de manera programada y con un fin en específico. Hoy en día, ha llegado a tal punto que ***Gartner*** [2] integra el concepto de tecnología de próxima generación como criterio fuerte a la hora de seleccionar este tipo de tecnologías en el mercado.

La idea principal de las tecnologías de próxima generación es buscar reforzar las falencias en seguridad que existen actualmente en las plataformas de primera

generación. Es tipo de tecnologías permiten implementar nuevas técnicas de adquisición de información de los ataques gracias a la globalización de casos conocidos donde se comparten información sobre nuevos malware, técnicas y comportamientos que son estudiados en laboratorios por grupos investigadores y comunidades de seguridad. Luego se brindan actualizaciones en tiempo real a las plataformas de próxima generación permitiendo estar a la vanguardia de los ataques y nuevas amenazas.

También los avances del malware han unificado en cierto modo a los fabricantes de tecnología de seguridad para que trabajen de manera "conjunta" logrando poder realizar investigaciones más profundas sobre malware recientes y análisis de código altamente desconocido como el mismo caso de Stuxnet. En este caso, los fabricantes como Karpersky unificaron fuerzas a nivel investigativo y analítico mediante foros/comunidades privadas, logrando compartir información sobre los avances del malware e ingeniera para el análisis complejo del código fuente.

La idea principal de esta investigación fue mostrar cómo estudiar y analizar ataques modulares utilizados por el malware avanzado para obtener fines específicos. Para ello, se utilizó tecnología de próxima generación a nivel perimetral que brindo información detallada sobre como son los ataques y sus metodologías dentro de la red. Inicialmente se realizó una investigación en base los diferentes tipos de empresas u organizaciones para conocer cuáles son sus principales servicios brindados y sobre que plataformas soportan este tipo de servicios.

Posteriormente se tomó información sobre como son las topologías y diagramas de red diseñados de clientes con los que he trabajado en base a mi experiencia laboral durante los últimos seis años. Estos diagramas contienen información visual de los clientes finales y solamente se utilizaron para soportar el conocimiento sobre que topologías e infraestructuras tecnológicas son utilizadas hoy en día de manera confidencial, también se realizaron encuestas detalladas de

manera anónima a empleados de diferentes sectores empresariales que trabajan en áreas afines a nivel de infraestructura, virtualización o seguridad informática, Además de coordinaciones y áreas de consultoría y auditoría para conocer en detalles sobre el compliance que rige en las empresas u organizaciones.

La encuesta ayudó a conocer de manera detallada información que no se pudo obtener a partir de los diagramas y topologías de red de ejemplo. Permitió además conocer más sobre que plataformas a nivel de seguridad existentes son utilizadas actualmente en las organizaciones empresariales y que tipo de actividades relacionadas con los servicios se encuentran en las empresas. Como parte complementaria ayudó a conocer si existen servicios particulares y plataformas virtuales dentro de las organizaciones actuales.

A continuación se detalla el tipo de estudios a realizado en base a la previa investigación redactada.

5 ESTUDIOS DE INFRAESTRUCTURAS DE REDES ACTUALES

5.1 INVESTIGACION DE TOPOLOGIAS Y DIAGRAMAS EXISTENTES EN REDES ORGANIZACIONALES Y CORPORATIVAS

Se realizaron los siguientes métodos de investigación para conocer las topologías actuales de las redes organizacionales y corporativas:

Encuesta Web: Se enfocó en conocer las topologías, infraestructuras y servicios en las redes de organizaciones actuales, consultando mediante de veinte (20) preguntas las cuales fueron respondidas por los encuestados de manera anónima, asegurando su confidencialidad.
Se encuestó alrededor de setenta (70) personas de diferentes países de la región las cuales ejercen diferentes tipos de cargos relacionados con la administración, coordinación, proyectos, consultoría, diseño, auditoria, etc, afines a las áreas de IT y SI. Tanto en el anexo II como en el siguiente link se puede visualizar la encuesta.

https://docs.google.com/forms/d/1mr1YJ30vTxlCMkq_IowMZXqdwl4gsyLuIcdDw_9hqD8/viewform

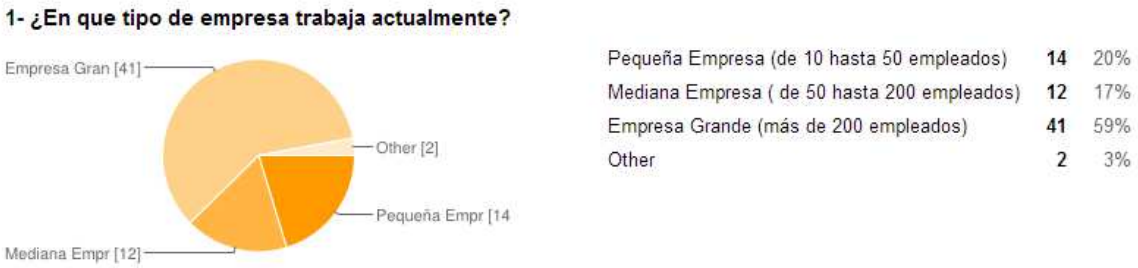
Estudio de topologías y diagramas esquemáticos de red: A diferencia de la encuesta, se analizaron topologías y mapas de red directamente de clientes con los cuales he trabajado a nivel de soporte, consultoría y dimensionamiento en networking y seguridad durante los últimos casi siete años de experiencia laboral. Estos datos NO son publicados dentro de esta investigación pero si referenciados debido a la sensibilidad de la información la cual manejan.

Otra fuente de información muy útil para conocer las topologías generales de las empresas actualmente son los fabricantes de tecnología de seguridad que

también soportaron información de cómo son las topologías típicas de sus clientes en base a sus soluciones para la simulación del laboratorio virtual.

5.2 RESULTADOS Y ESTADISTICAS ENCUESTAS:

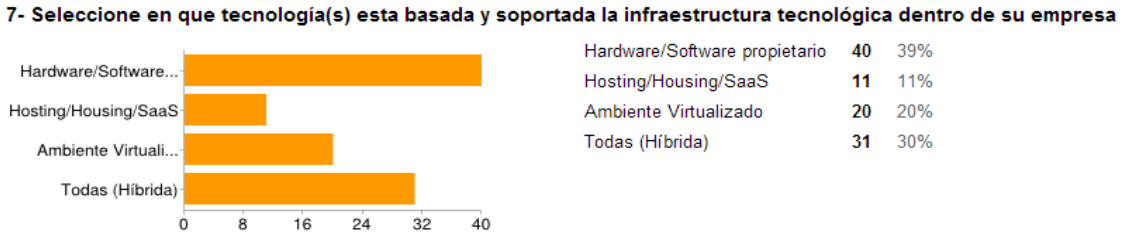
En base al relevamiento de los resultados de la encuesta, se puede deducir que casi el 60% de los encuestados indican que trabajan en empresas donde cuentan con más de doscientos (200) empleados. Los datos de las siguientes graficas 1 y 2 corroboran que la mayoría son empresas grandes y corporativas (dependiendo los tipos de empresas dependiendo el sector).



Gráfica 1. Tipos de empresa

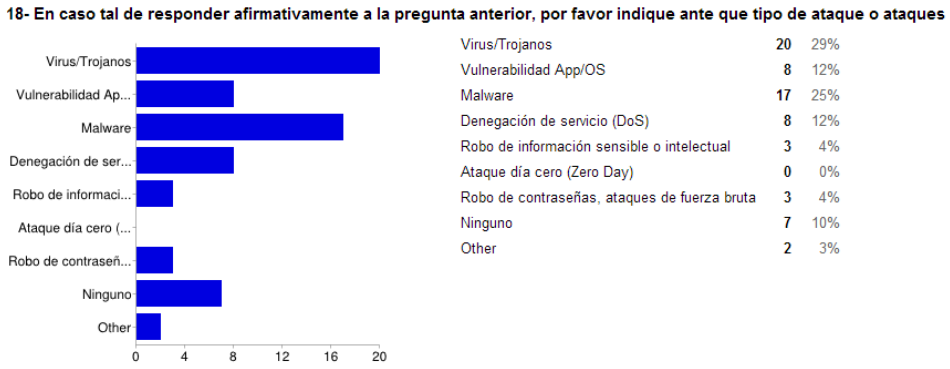
Gráfica 2. Sector empresarial

Se pudo notar que la mayoría brinda servicios corporativos junto a la banca, comunicaciones y tecnología. Alrededor del 32% de empresas se encuentran trabajando en sectores diferentes.



Gráfica 3. Tipos de infraestructuras

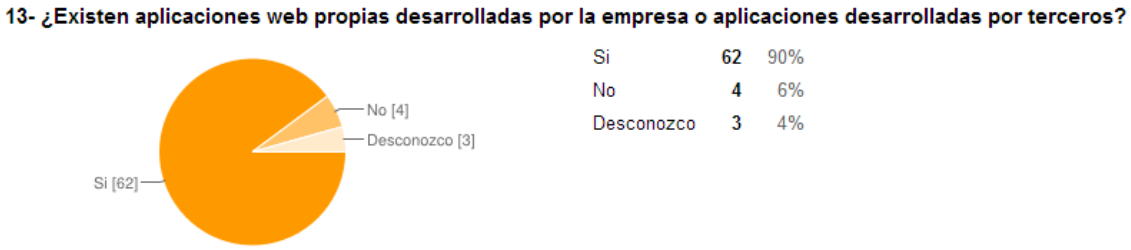
Si bien aún se mantiene en un gran porcentaje la infraestructura física a nivel de hardware y software (casi un 40%), el 30% de las empresas hoy en día se complementan utilizando infraestructuras hibridas (físicas y virtuales) para soportar y brindar recursos en su infraestructura tecnológica. También en un bajo porcentaje, se puede notar que algunas cuentan con servicios tercerizados en la nube y servicios tipos SaaS (11%).



Gráfica 4. Tipos de ataques.

En la gráfica 4. Se puede ilustrar la mayoría de incidentes de seguridad. Los encuestados confirmaron que la mayoría de ataques recibidos en sus empresas están relacionados a vulnerabilidades, virus, troyanos o malwares asociados (64%), es curioso notar que si bien se confirman ataques a vulnerabilidades, nadie asocio este tipo de incidentes a los ataques día zero los cuales tienen una fuerte relación debido al desarrollo propio de software por parte de las organizaciones, incluso el

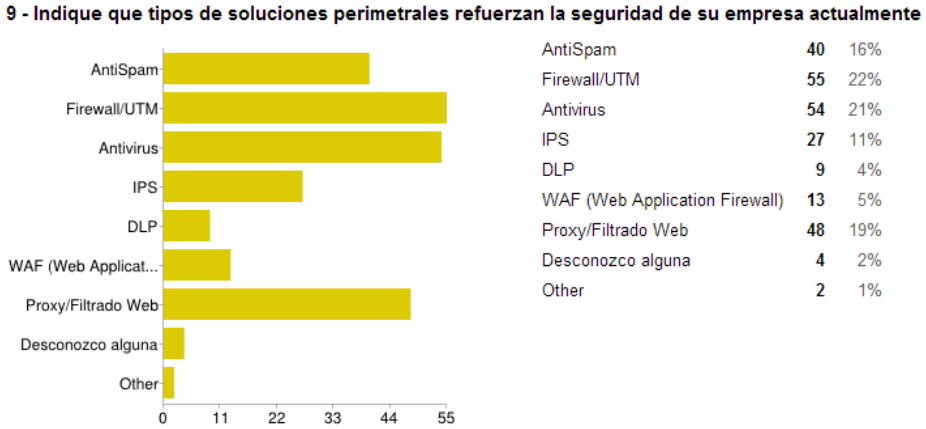
90% de los encuestados confirmó que este tipo de desarrollos existe o por terceros en sus organizaciones (Grafica 5).



Gráfica 5. Desarrollo web de aplicaciones

Gráfica 6. Servicios encuestados

La grafica 6 ilustra los servicios brindados a nivel de networking y seguridad por parte de las empresas.



Gráfica 7. Infraestructura de seguridad

La grafica 7 ilustra la seguridad de primera generación existente en las organizaciones. Las tecnologías principales para la protección se encuentran en el control de navegación de usuarios (Proxy), firewalls perimetral, sistemas de prevención de intrusos (IPS) y protección de servicios de correo electrónico.

5.3 CONCLUSIONES SOBRE LAS INVESTIGACION DE INFRAESTRUCTURAS

Luego de los resultados de la investigación y teniendo en cuenta la tendencia de las tecnologías utilizadas por las empresas y sus servicios implementados en base su arquitectura de red, se implementó la topología de red seleccionada para el ambiente virtual de laboratorio.
A continuación se listan el toplist de servicios que fueron implementados dentro del ambiente, gracias a los estudios realizados previamente.

- **Correo (SMTP)**
  Servidor Windows 2003 – Software de Correo Kerio Connect

- **Navegación/Intranet (HTTP/HTTPS)**
  Firewall Checkpoint URL Filtering / Gaia R77.10
  File Server 2003 SP1

- **Conexión Remota (RDP/VPN)**
  Firewall VPN SecureRemote Checkpoint /R77.10
  Servicios de RDP activados en servidores Windows 2003 SP1

- **Servicios de Directorio (DC,LDAP,DHCP,DNS)**
  Servidor Windows AD 2003 SP1, DNS, DCHP roles activados

- **Servidor de Archivos/BD (NFS,SQL)**
  Servidor Windows 2003 SP1 MS SQL Server 2008

En base a los resultados estadísticos de la encuesta se simularon las siguientes soluciones y dispositivos de seguridad de primera generación:

- **Solución de Firewall**
  Checkpoint R77.10 GAIA
- **Solución de Filtrado Web**
  Checkpoint R77.10 GAIA URL FILTERING
- **AntiSpam**

KERIO CONNECT MAIL SERVER

- **IPS**

Checkpoint R77.10 GAIA IPS BLADE

Nota: Si bien el Antivirus fue la solución de seguridad con un altor porcentaje, en la encuesta solo se tuvo en cuenta para fines investigativos. Se evitó simular dentro de la PoC este tipo de protección en las maquinas finales debido a que esta investigación NO apunta al estudio del comportamiento del código de malware en clientes finales, omitiendo todo tipo de análisis y orientando en mayor detalle el análisis al comportamiento del malware avanzado dentro de la red.

6 ANALISIS DEL MALWARE AVANZADO

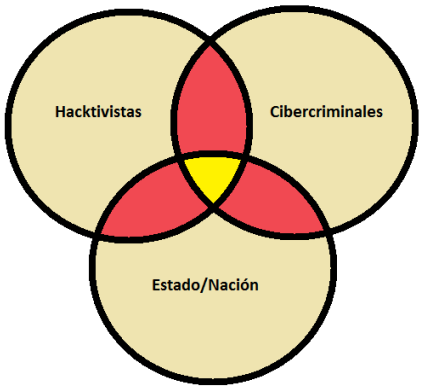
DESARROLLO DE NUEVOS VECTORES DE ATAQUES – REDES SOCIALES.

Actualmente debido a la convergencia de servicios en las grandes redes, los desarrolladores de malware han trabajado en métodos prácticos para la creación de nuevos vectores de ataques. Aprovechan las nuevas tendencias del mercado empresarial como por ejemplo, aquellas empresas que utilizan herramientas como las redes sociales en las áreas dentro de la organización y así poder infiltrar malware a usuarios que tienen permisos de navegación a las redes sociales.

Por ello, es importante reconocer que los atacantes buscan desarrollar nuevas técnicas de malware o a través de ingeniera social obtener la mayor información de empresas que exponen sus datos e información en redes sociales. Otro ejemplo es el tipo de infraestructuras ofrecidas actualmente como los sistemas de VDI (Virtual Desktop Infraestructure) brindando múltiples acceso a aplicaciones desde un escritorio virtual. Este tipo de plataformas han sido implementadas en los últimos años por las organizaciones como demuestran las encuestas realizadas donde respondieron que un 7% de estas brindan este tipo de servicios en sus plataformas actuales. (Destacado en punto 2 en la gráfica 6 del capítulo 5).

Las infraestructuras nuevas permiten que las redes actuales se flexibilicen creando nuevos retos de seguridad para los administradores de las plataformas que deben analizar los accesos de usuarios y cómo interactúan estos con los servicios y aplicaciones. Un ejemplo puede ser la navegación Web a sitios permitidos relacionados a redes sociales o sitios desconocidos. No obstante este no es el único reto que enfrentan, sino también se encuentran ante la tentativa de poder brindar servicios para dispositivos móviles dentro de la red utilizando conceptos como BYOD que ha sido llevado a las empresas en la actualidad.

Estas igualmente tratan de mitigar las posibles amenazas y riesgos en las conexiones de los dispositivos móviles hacia las aplicaciones utilizando herramientas tipo MDM para aplicar controles a los accesos por parte de los dispositivos móviles[2].



Gráfica 8. Grupos atacantes

Otro de los grandes retos de seguridad que enfrentan las empresas debido al crecimiento de las organizaciones, es implementar nuevas tecnologías convergentes que estén a la vanguardia de los cambios y ataques que enfrentan las organizaciones por parte de hacktivistas, cibercriminales y desarrollos patrocinados por gobiernos o naciones. El punto crítico y el reto de toda organización es brindar seguridad que enfrente este tipo de amenazas que convergen en la zona amarilla ilustrada en la gráfica 8.

A continuación se describen los tres retos principales que enfrentan cada área de seguridad informática en distintas organizaciones tratando de ir acorde a las políticas de seguridad y dependiendo de sus áreas de negocio:

[2] Documento John Yamich and Anthony Smith - Anonymous and LulzSec: The impact hacktivist organizations have on our perceptions of hackers and information security.

- **Las amenazas crecen exponencialmente:**

Cada día evolucionan las nuevas amenazas por parte de los atacantes, es conocido que los ataques de los cibercriminales buscan objetivos puntuales y no diversos. La evolución de algunos grupos hacktivistas como ***Lulzec*** y ***Anonymous,*** los cuales se han especializado en realizar ataques puntuales utiliza métodos de dispersión como los *DDoS*. Las empresas deben concientizarse de los ataques puntuales o individuales los cuales los hackers centran su atención.

- **Evolución de la Infraestructura Tecnológica**

Gracias a las encuestas y los resultados, estos indican que los servicios en la nube, ambientes de virtualización, tecnologías BYOD, aplicaciones móviles, redes sociales, etc. son muestras de la real transformación y evolución de las infraestructuras tecnológicas hoy en día. Esto va de la mano a que los nuevos modelos de infraestructura suman complejidad tecnológica y tienden a ser un reto para los CISOs siendo estos los principales responsables de idear la conducción de políticas de seguridad alineadas a las intereses de la empresa, manejar proactivamente la seguridad de la información e inclusos los riesgos a nivel estratégico en base a los cambios de IT.

A medida que aumentan los recursos que brindan disponibilidad a los usuarios en la infraestructura aumentan las amenazas y vectores de ataque, las nuevas tecnologías traen complejidad al contexto existente de las redes y la complejidad, es uno de los mayores enemigos para la seguridad.

- **Regulaciones y normativas:**

En la actualidad ante las regulaciones y normativas actuales para el manejo de información y datos, no simplemente es traer la seguridad ante estos escenarios sino que también las empresas buscan cumplir las normativas las cuales rigen en base al sector en el cual se desempeñan, pero también teniendo en cuenta múltiples variantes como conflictos en las directivas de regulación entre áreas y los problemas internos industriales no existe una forma exacta para que las organizaciones puedan tener éxito en la aplicación de regulaciones vigentes.

La complejidad de las infraestructuras actuales vuelve más difícil el escenario para cumplir estas directivas que aseguran que las organizaciones se encuentren al día con las regulaciones, porque no solamente debe ser aplicadas empresarialmente estas sino también deben encontrar formas para implementar las políticas, análisis de riesgo y frameworks de cumplimientos en sus partners, servicios de outsourcing o tercerizados y clientes vigentes.

El resultado de esto puede ser insatisfactorio en algunos casos, obviamente las organizaciones pueden ser muy predecibles al aplicar los guidelines de implementación para el complicance, algo que los atacantes también pueden conocer.

6.1 INVESTIGACION DE MALWARE AVANZADO SOBRE PLATAFORMAS EXISTENTES

- **FLAME (También conocido como Skywiper – Flamer)**

Flame (Skywiper) es uno de los malware más avanzados generando mucha preocupación en los principales fabricantes y consultores a nivel de seguridad. La forma que fue desarrollado a través de una arquitectura modular casi perfecta en

diseño y como utiliza los recursos físicos y lógicos en las máquinas infectadas asombra a comparación de sus predecesores.

Flame utiliza y combina ataques conocidos y técnicas utilizadas por otros códigos maliciosos lo que inmediatamente lo catalogo como un *blended threat*. Otras de las grandes singularidades de Flame es su forma de poder manipular desactivando y activando sus módulos internos de su código dependiendo del ambiente de red donde se encuentre. Esto convierte a Flame en un malware inteligente con capacidad de adaptación y evolución dependiendo del ambiente.

A continuación se describen cada uno de los módulos de Flame, además se brinda un detalle resumido del comportamiento de cada uno de ellos.

- **Beetlejuice:** Módulo utilizado para la propagación del código. También es visto como uno de sus métodos más eficaces automatizados ya que puede activar el dispositivo Bluetooth en la maquina infectada y colocarla como un dispositivo descubrible. Luego cuando los dispositivos dentro de su rango se conectan a la maquina infectada esta codifica el código principal utilizando codificación ***Base64*** para posteriormente enviarlo a la maquina target.

- **Microbe:** Este módulo está encargado de grabar todo sonido receptado por la máquina a partir de los dispositivos de recepción de audio locales. Una vez detecta todos los dispositivos que existen en la máquina, lista cuales se encuentran activos y disponibles para grabar, posteriormente elige uno de estos para poder grabar información y luego ser enviada al atacante.

- **Infectmedia:** Encargado de seleccionar uno de los métodos para infectar los dispositivos por ejemplo a través de disco duros externos. Los métodos disponibles utilizados son *Autorun_infector* o *Euphoria.*

- **Autorun_infector:** Este módulo crea el archivo autorun.inf, dependiendo del modo de infección utilizado anteriormente. Este archivo contiene en si el código de malware y comienza con el *open command Euphoria*.

- **Limbo:** Crea puertas traseras (backdoors) en el sistema utilizando la cuenta "*HelpAssistant"* siempre y cuando la maquina se encuentre en el dominio y tenga permisos necesarios para crearla.

- **Frog:** Modulo encargado de infectar la maquina objetivo utilizando cuantas de usuarios previamente establecidas. La cuenta establecida en la configuración del recurso es "*HelpAssistant"**,*** creada utilizando el método Limbo.

- **Munch:** Este módulo crea un HTTP Server en el paciente cero para poder ser utilizado en la replicación de malware en las máquinas de la red. Responde a las solicitudes */view.php* y */wpad.dat*.

- **Snack:** Este módulo escucha todas las interfaces de red disponibles, recibe y graba los paquetes NBNS proveniente de los dispositivos y luego los almacena en un archivo de Log. Tiene la opción de solo ser activado una vez comienza a correr el módulo *Munch*.

- **Boot_DLL_Loader:** Es una de las DLL instaladas por el malware para recolectar información en modo de lista. También contiene información de todos módulos que deberían estar cargados y activos dependiendo del ambiente.

- **Weasel:** Crea una directorio donde lista todos los computadores, servidores y dispositivos infectados.

- **Boost:** Crea una lista de archivos interesantes para el malware los cuales son enmascarados con diferentes tipos de nombres.

- **Telemetry:** Encargado de facilitar el logging de eventos para cada uno de los módulos.

- **Gator:** Cuando una conexión de internet se encuentra disponible, automáticamente el modulo intenta comunicarse con los servidores CnC de tal forma que pueda descargar nuevas actualizaciones de código e instrucciones de comando y subir información referente a sus actividades.

- **Security:** Es el encargado de identificar todos los programas de seguridad en los dispositivos, máquinas y servidores que puede detectar o analizar Flame. Contiene submódulos y rutinas avanzadas para evadir la detección por parte de tecnología local de seguridad.

- **Gadget:** Extiende la propagación en la red desde una maquina infectada o bot (diferente a la maquina paciente cero) hacia otra nueva máquina a infectar.

Una característica fuerte sobre la arquitectura modular de Flame es permitir que el comportamiento del malware adopte ciertas variantes en base a los módulos que se activan, de esta forma poder llegar al objetivo o a la información que se desea obtener. Flame también puede realizar actualizaciones sobre su código y enviar información a los servidores CnC externos sin ser detectado a través de múltiples conexiones con diferentes protocolos de red. Las características de Flame serán simuladas dentro de la PoC con diferentes ejemplos de malwares estudiados para estudiar el comportamiento del malware una vez se encuentra en la red y como se puede radicar detectando el paciente cero el cual contiene el código principal del malware y siendo la raíz de propagación de este.

Las amenazas mezcladas o *blended threats* inicialmente eran conocidas como *computer threats* pero a medida que los desarrolladores de malware han incorporado nuevas técnicas, la idea principal es que los objetivos del malware sean alcanzados en una mayor probabilidad cuando se realiza el ataque.

Este tipo de técnicas son utilizadas por Flame, donde según el reporte de seguridad realizado por *Eric Usher* en el documento *Flame Malware Analysis* indica que otra de las fuertes propiedades del código, es utilizar el módulo de Security para correr rutinas que permitan colocar el malware en modo sleep y así evitar ser detectado. A continuación se detalla parte del texto en las conclusiones finales de su estudio:

"De acuerdo con la compañía llamada GFI, Flame esta prevenido ante ambientes virtualizados ya que utiliza la técnica de sleep para prevenir el análisis realizado en máquinas virtuales. Flame utiliza varias funcionalidades de hibernación como método principal para no ser detectado por emuladores y ambientes virtuales, no hace nada a menos que este fuera de este tipo de ambientes[3]"

Como conclusión, debido a este comportamiento intrínseco de Flame se opta por simular el comportamiento de los módulos de malware de Flame utilizando otros malwares que permitieron visualizar y simular su comportamiento similar para la detección.

[3] Texto tomado y traducido directamente del reporte de *Flame Malware Analysis* por *Eric Usher – Champlain College*

6.2 OBTENCION DE TECNICAS Y METODOS DE ATAQUES DE MALWARE A UTILIZAR MEDIANTE EL ESTUDIO PREVIO DE ATAQUES

Una de las limitantes actuales para poder simular Flame en ambientes virtualizados, honeypots o utilizando técnicas de sandboxing, es su técnica de evasión y detección que posee utilizando metodología tipo rookit en su módulo ***"Security"***. Debido a esto, se optó por utilizar dos malware conocidos y poderosos actualmente en el mercado que presenta este tipo de características parecidas a Flame.

Como criterio de seguridad inteligente, las herramientas de seguridad utilizadas en la prueba de concepto poseen técnicas de sandboxing como uno de los tantos criterios de seguridad para la detección de malware. Gracias a los avances que han aportado las técnicas de sandboxing, exploradores Web como Chrome han utilizado este tipo de tecnologías inicialmente. Este tipo de técnicas también son utilizadas por software Open como ***Cuckoo Sandbox***, el cual realiza sandboxing de dispositivos que en ambientes aislados y brinda reportes de comportamiento del malware en ambientes locales [6].

Uno de los objetivos principales de la prueba de concepto, es poder contar con muestras de malware que simularon técnicas parecidas a los módulos utilizados por Flame descritos anteriormente. Esto permitió analizar el comportamiento dentro de la red y se pudo visualizar como una maquina pudo introducir malware en la red convirtiéndose en el paciente cero de propagación. De esta forma que se pudo evaluar la trazabilidad en la transmisión de malware y obtener un espectro de infección.

A pesar que a continuación se utilizaron y presentaron ejemplos de malwares los cuales tuvieron un impacto fuerte dentro de las redes organizaciones, estos ya han sido investigados y solventados por diferentes investigadores y fabricantes de seguridad. La principal idea fue recrear el comportamiento del malware en la red

dentro de la red y que técnicas son utilizadas para lograr su objetivo específico. Por otra parte, los sistemas operativos utilizados en las pruebas de concepto se basaron en las siguientes plataformas de Windows:

- **Windows Server 2003 SP2** (Actualizaciones inhabilitadas)
- **Windows XP Professional SP2** (Actualizaciones inhabilitadas)
- **Windows 7** (Actualizaciones inhabilitadas)

Ninguna plataforma contó con seguridad local a nivel de políticas ni antivirus, ya que como se explica en las conclusiones del capítulo 5 el objetivo principal no se enfocó en el estudio del malware en máquinas finales e infectadas.

A continuación, se listan los malwares utilizados en las pruebas en las pruebas de concepto y se describen como ejemplo algunas vulnerabilidades relacionadas a estos.

- ***WIN32/Palevo***

  Malware tipo gusano detectado en Julio 23/2009. Este malware se destaca en afectar sistemas (Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows Server 2008, Windows Vista, Windows X) realizando exploits sobre las siguientes vulnerabilidades descritas en las publicaciones del CVE:

  CVE-2003-0352

  La vulnerabilidad permite realizar un buffer overflow en una de las interfaces de DCOM del RPC en sistemas como MS Windows NT 4.0, 2000, XP y MS Server 2003. Los atacantes remotos pueden ejecutar código malicioso realizando *exploit*s que son activados por gusanos de diferentes clases y variantes [7].

CVE-2005-0059

A través del componente de Message Queuing de MS Windows 2000 y Windows XP SP1, se puede realizar un Buffer Overflow permitiendo a los atacantes ejecutar código malicioso mediante mensajes especialmente diseñados para el exploit [8].

- ***Back.tidserv o Win32/Alureon***

Malware troyano detectado en Septiembre del 2008, muy conocido también como ***Alureon.*** Este troyano con capacidad de autocultamiento utiliza avanzadas técnicas de rootkit para evitar ser detectado por sistemas de seguridad locales. Puede redireccionar el tráfico de consultas de los usuarios y abre backdoors en las máquinas infectadas.
Este malware es catalogado como un ***blended threat*** por sus propiedades intrínsecas que afectan sistemas tipo Windows 2000, Windows NT, Windows Server 2003, Windows Vista, Windows XP.

A continuación se listan algunas de sus vulnerabilidades conocidas y reportadas por el CVE:

CVE-2013-3897

Vulnerabilidad en la clase ***CDisplayPointer*** librería del archivo mshtml.dll utilizada por los exploradores de Microsoft Internet desde la versión 6 hasta 11. Permite a los atacantes remotos ejecutar código en específico o causar un ataque tipo DoS (corrupción de memoria) utilizando mensajes de JavaScript diseñados especialmente para utilizar la propiedad *onpropertychange* del event handler. La vulnerabilidad también es conocida como “Internet Explorer Corruption Vulnerability” [9].

CVE-2011-3544

Vulnerabilidad no especificada en el Java Runtime Environment Component en Oracle para las versiones Java SE JDK y JRE 7 y 6 Update 27 y versiones anteriores. A través de esta se permite controlar remotamente aplicaciones tipo Java Web y Java applets no confiables afectando la confidencialidad, integridad y disponibilidad de datos mediante vectores de ataque desconocidos relacionados al scripting [10].

Si bien se utilizaron variantes de estas dos muestras de malwares para las pruebas de concepto descargadas directamente del sitio ***www.offensivecomputing.net,*** existieron limitantes de su comportamiento al momento de interactuar con las vulnerabilidades relacionadas o con las acciones que realizan para lograr su objetivo. La idea no fue estudiar directamente los casos conocidos sobre las vulnerabilidades sino estudiar el comportamiento de este tipo de malwares que realizan otros tipos de exploits y comportamientos en la red una vez se encuentran infectado los sistemas.

El análisis que se enfocó a la problemática inicialmente planteada a través de la prueba de concepto apuntará directamente al comportamiento del malware en la red una vez transmitido y ejecutado en las máquinas, validando que tipo de conexiones y métodos a nivel de tráfico utiliza para poder ser detectado sin necesidad de realizar un análisis profundo en las máquinas directamente infectadas.

7 PRUEBAS DE CONCEPTO

El objetivo principal de la prueba de concepto es analizar, detectar e investigar en un ambiente real controlado el comportamiento del malware en la red. Luego de analizar los estudios de topologías típicas de los clientes, se diseña una red que contenga la misma cantidad de servicios elegidos montando las máquinas y servidores dentro del ambiente para simular el escenario elegido.

A continuación se listan los pasos realizados para llevar a cabo la prueba de concepto de malware en la topología de red simulada.

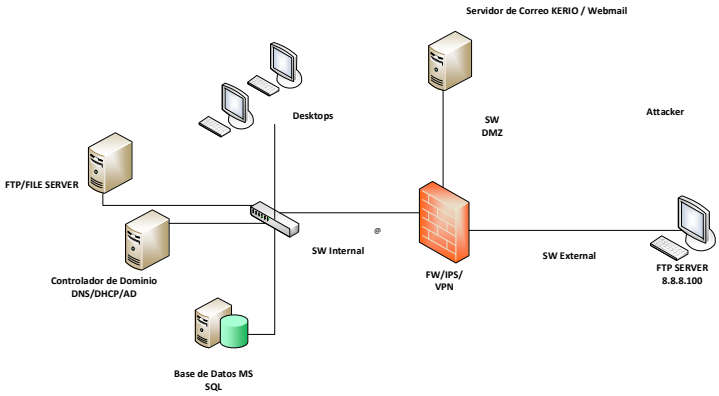


Figura 3. Topología de red propuesta para montaje de PoC

7.1 Montaje y configuración de la topología de red estudiada en la plataforma VMWARE ESX 5.5

Para el montaje del laboratorio, se explica que recursos fueron utilizados a nivel físico y lógico para la simulación de la red especificando como fueron asignados a cada de las máquinas, dependiendo del consumo que realizada cada una de estas para la prueba. Posterior a esto se

realizaron instalaciones de sistemas operativos, software, y configuraciones sobre los servidores para las conexiones, simulando todos los recursos de toda la topología.

Una vez las máquinas y servicios se encuentran montados, se procedió a realizar las conexiones lógicas entre los switches virtuales para las conexiones entre los equipos y los segmentos de red utilizando tecnología de primera generación como el virtual appliance de firewall. Para comunicar todas las redes, se conectaron los segmentos de red internos al módulo de la tecnología de próxima generación que interceptó el tráfico de manera intrusiva o en “modo inline”.

Máquina	**Zona de red**	**Descripción de servicios**
Servidor de correo	DMZ	Servicios de correo SMTP y correo webmail para usuarios del dominio
Controlador de dominio	Interna	Servicios de directorio, resolución de nombres y DHCP
Servidor de base de datos	Interna	Servicios de base de datos a través del motor de SQL
Servidor de archivos compartidos	Interna	Servicios de FTP, archivos compartidos y motor de aplicaciones web
Máquinas victimas	Interna	Máquinas con servicios de escritorio y acceso a usuarios del dominio
Máquinas atacante	Externa	Máquina desde la cual se realiza la infección a máquinas del dominio
Sensor de Malware	Seguridad	Consola y sensor para la detección y análisis de malware y ataques en la red
FW/IPS/AntiSpam	Seguridad	Seguridad de primera generación Firewall, IPS, filtrado Web y Antispam

Tabla 1. Inventario de máquinas activas en laboratorio

7.2 Infección de toda la topología de red virtualizada

Una vez montada la topología y conexiones se realizaron las infecciones sobre las maquinas utilizando el protocolo de transferencia de archivos FTP para transmitir el código malicioso a las máquinas internas. Luego el malware fue ejecutado en las máquinas elegidas e inicialmente se dejó el malware un sobre la red durante un tiempo aproximado prologando para analizar su comportamiento sobre la infraestructura virtual.

7.3 Análisis de malware a través de los eventos y logs del tráfico.

Tal como se concluye al final del capítulo 5, no se simuló la protección a nivel de antivirus para esta prueba de concepto. Si bien esto no interfiere con los objetivos de la PoC, la idea principal es que las muestras de malware a utilizar no se vieran limitadas por el antivirus independientemente de su comportamiento.

7.4 Análisis de espectro

Por último se realizó un análisis del espectro de los archivos transmitidos por la maquina atacante a través del protocolo FTP y que archivos fueron transmitidos directamente por el malware. Se replegaron utilizando este protocolo de transmisión.

7.5 Hallazgos y resultados

Uno de los ejemplos directos de comportamiento de malware en la red que pudo evidenciarse dentro de la prueba de concepto fue el caso de la variante de malware Palevo, el cual realizaba desde el controlador de dominio un escaneo de puertos sobre el Gateway para conocer qué servicios o puertos

estaban abiertos, de tal forma, que esta información sea utilizada por el malware para realizar conexiones tipo CnC desde la maquina o maquinas infectadas. Básicamente fue un ejemplo de cómo interactúan y aprenden los malwares sobre el contexto de la red utilizando técnicas como el *portscan,* en este caso para conocer información referente a exposiciones y reglas permisibles en los equipos de seguridad como el firewall y así aprovechar este tipo de brechas como parte de su actividad.

Si bien no existió conexión directa entre el laboratorio e internet, se pudo ver que la variante de Alureon buscaba la forma de poder comunicarse a cierto pool de direcciones detectadas por el *"Geolocalition"* las cuales tienen destino a los servidores CnC en distintos países. Este método de contacto surge debido a que los atacantes una vez infectadas las maquinas no pueden iniciar la conexión directamente desde su origen, ya que las maquinas internas no están publicadas para poder ser controladas por el atacante.

Estas es una de las más innovadoras técnicas por parte de los atacantes y malwares creadores de bots, la cual consiste en realizar la conexión con los servidores iniciando de manera automática cualquier tipo de comunicación desde la red interna hacia el servidor. Para lograr esto, infectan las maquinas creando bots o una botnet los cuales utilizan diferentes protocolos de conexión posiblemente permitidos como la navegación a redes públicas o conexiones utilizadas por otros servicios internos que estén habilitadas en el firewall de manera general.

No obstante, el malware cuando se encuentra en la red puede utilizar protocolos distintos transmisión de archivos como FTP o de aplicación conocidos como *HTTP, HTTPS, SMB, POP3, SMTP* entre otros o incluso utilizar técnicas de propagación como los gusanos o vulnerabilidades de ciertas aplicaciones o sistemas base.

Se pudo detectar comunicaciones anómalas o por ejemplo intentos no típicos de conexión tipo DNS hacia servidores externos puntuales. El malware trató de establecer comunicaciones con servidores que están catalogados como dominios de malware como lo es ***jabena.ananikolic.su***. Este tipo de detección permitió identificar que a pesar de que las solicitudes de sincronización de dominios pueden ser válidas dentro de la red desde un controlador de dominio hacia internet, el malware que reside en el servidor de DNS trata de sincronizar la tabla local con utilizando estos sitios maliciosos. La variante del malware Palevo utiliza este método para desviar las comunicaciones de las maquinas clientes una vez estas tratan de consultar sitios para la navegación en un servidor de DNS comprometido.

8 METODOLOGIA DE IMPLEMENTACION PLATAFORMA DE PROXIMA GENERACION EN LAS REDES ACTUALES

A continuación se describirán recomendaciones para la implementación de tecnología de próxima generación partiendo de la experiencia, los resultados de los estudios realizados y la prueba de concepto.

Las siguientes preguntas utilizadas en la encuesta realizada también pueden ser consultadas como base para indagar sobre la topología de las organizaciones actuales:

1- ¿Qué tecnología o tecnologías son soportadas en la infraestructura tecnológica dentro de la empresa?
2- Dentro de la infraestructura tecnológica de la empresa, ¿qué tipo de conexiones se permiten a nivel inalámbrico para las áreas de trabajo y acceso a internet?
3- Indique que tipos de soluciones de seguridad perimetrales, en usuarios finales y servidores refuerzan la seguridad de su empresa actualmente.
4- Que servicios a nivel de hosting/housing/SaaS han sido contratados a nivel de seguridad
5- Listar que servicios a nivel de networking y seguridad se brindan en su empresa
6- ¿La empresa cuenta con certificaciones en seguridad para sus procesos internos y externos a nivel de compliance?
7- ¿La empresa permite conexiones de dispositivos móviles y tablets estilo BYOD para las aplicaciones web internas o publicadas?
8- Listar que redes sociales son permitidas comúnmente para los usuarios dentro de su empresa

9- ¿Existen soluciones tipo SIEM (Security Information and Event Management) en la infraestructura de seguridad de la empresa?

También es necesario detallar la siguiente información en lo posible a nivel de servidores y maquinas internas dentro de la red, como se muestra en la tabla 2.

Usuarios y Máquinas
Número de Máquinas
Usuarios de VDI
Usuarios de Aplicación
Usuarios de VPN
Usuarios de Navegación
Servidores Web
Servidores de Aplicación
Dispositivos Móviles
Máquinas de usuarios

Tabla 2. Lista de inventario usuarios y máquinas.

Se debe realizar un estudio de la cantidad de redes que segmentan a los servidores, dispositivos de conexión y soluciones de seguridad existentes en la topología de la empresa como lo indica la siguiente tabla.

Tipos de segmentos de red
DMZ
Interna
Externa
WAN
VLAN

Tabla 3. Lista de tipos de segmentos de red

El estudio de conocimiento sobre la cantidad de segmentos de red que existe dentro de la topología, busca interceptar el tipo de tráfico el cual está relacionado con el posible comportamiento del malware en caso de existir y permite analizar a la herramienta de seguridad de próxima generación.

La tecnología de próxima generación busca interceptar el tráfico de los segmentos los cuales inspeccionan todo el tráfico de red. La mejor forma y la más recomendada para este tipo de tecnologías es la implementación del “modo inline”, razón por la cual es necesario el dimensionamiento del número de segmentos que existen y va relacionado a las características físicas y de recursos del equipo que analizará todo el tráfico por segmento de red definido.

Para los ambientes virtuales, es necesario estudiar dependiendo qué tipo de fabricante o plataforma de seguridad va a ser utilizada (ya sea opensource o comercial) en la implementación como tecnología de próxima generación. Existen en la actualidad plataformas como Hipervisor o ***Hiper-V*** que facilitan dependiendo el contexto de red existente en las organizaciones utilizar y soportar tecnologías de próxima generación para ambientes híbridos o netamente virtuales.

9 CONCLUSIONES

Los resultados de la investigación y la prueba de concepto realizada, nos permite afirmar que es importante contar con tecnología de próxima generación para contrarrestar y mitigar las nuevas técnicas de ataque.
Esta tecnología ayuda a visualizar, detectar y realizar trazabilidad del malware en la red, ante los nuevos vectores de ataques introducidos por los desarrolladores de malware que cada vez usan algoritmos más sofisticados para poder introducirse en las redes actuales evadiendo la seguridad de las redes organizacionales.

Mediante los resultados de la encuesta a los involucrados (técnicos, administradores, coordinadores y consultores) sobre sus organizaciones, pudimos determinar que actualmente solo el 40% de los casos consultados cuenta con tecnología para proteger la red ante ataques de malware avanzado, lo cual nos permite afirmar que actualmente en la región pocas empresas son conscientes sobre los posibles ataques a los cuales se encuentran expuestas.

El estudio de topologías de ejemplo tomadas de diferentes empresas, nos hace ver que las redes son complejas en cuanto a sus conexiones de infraestructura e involucran tecnologías como escritorios virtuales, virtualización de servidores, herramientas de alta disponibilidad, etc. que incrementan aún más la complejidad.
Esto es debido a la necesidad de brindar servicios en distintos sitios, outsourcing a clientes y a la necesidad de poder contar con IT para brindar una alternativa de continuidad de negocio.
Esta complejidad además trae como consecuencia que las infraestructuras actuales sean difíciles de visualizar completamente, lo cual en algunos casos hace que no se puedan entender y esto hace que aumente la dificultad de darles seguridad.

Como vimos en el trabajo, al momento de implementar tecnología de próxima generación para el análisis de malware es necesario conocer varios puntos sobre la topología que se desea analizar en específico. Un elemento importante es determinar la posibilidad que el malware ya se encuentre en la red y tratar de conocer el primer equipo infectado o paciente cero y si el malware se está propagando o comunicándose utilizando las técnicas discutidas.

Es importante reconocer que la tecnología de próxima generación no busca reemplazar de manera determinante la tecnología de primera generación sino complementarla para que ayude a reforzar con nuevas técnicas de detección.
Un ejemplo de lo dicho son los antivirus, en la primera generación el análisis se realizaba localmente sobre las máquinas y en esta tecnología se realiza como un servicio de seguridad en la red.

Como vimos, la convergencia de servicios y topologías hibridas en la nube permiten que las tecnologías de seguridad se actualicen brindando protección a las redes ante ataques como día zero.
Un elemento que dificulto el trabajo fue que existen malwares como el FLAME estudiado en este proyecto que cuentan con módulos que tienen técnicas de ocultamiento para no ser detectados en ambientes virtuales, esto se solvento utilizando muestras de malware como ALUREON y PALEVO que presentan un comportamiento similar pero que no poseen las técnicas de ocultamiento. En el trabajo pudimos evidenciar las conexiones a los nodos externos (conexiones tipo CnC) que son similares a las utilizadas por FLAME.

Como resultado del estudio y análisis del presente trabajo, se pudo cumplir con el objetivo de elaborar una guía para la implementación de seguridad utilizando tecnologías de próxima generación que permiten mitigar el riesgo que producen las técnicas de malware actuales.

10 BIBLIOGRAFIA

[1] Flame Virus Cyber Warhttp://rt.com/news/flame-virus-cyber-war-536/(Consultada el 21/05/2014)

[2] PushDo malware resurfaces with DGA capabilities, http://threatpost.com/pushdo-malware-resurfaces-with-dga-capabilities. (Consultada el 09/07/2013)

[3] Advanced Malware, Targeted Attacks Compromise Enterprises via 'Security Gap'. (Consultada el 09/07/2013)

[4] Advance malware targeted attacks http://www.eweek.com/c/a/Security/Advanced-Malware-Targeted-Attacks-Compromise-Enterprises-via-Security-Gap-622155/ (Consultada el 24/10/2013)

[5] What is a blended threat? http://searchsecurity.techtarget.com/definition/blended-threat (Consultada el 24/06/2014)

[6] Cuckoo Sandbox, http://www.cuckoosandbox.org/. (Consultada el 09/02/2014)

[7] CVE-2003-0352, http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-0352. (Consultada el 24/06/2014)

[8] CVE-2005-0059, http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-0059. (Consultada el 24/06/2014)

[9] CVE-2013-3897, https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3897. (Consultada el 24/06/2014)

[10] CVE-2011-3544, https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3544. (Consultada el 24/06/2014)

[11] Do you need “Advanced Malware Protection” from 0days and the APT? Key Economic Considerations, http://spiresecurity.com/?p=1362 (Consultada el 12/09/2013)

[12] Virtualización de redes, http://www.luisespino.com/pub/virtualizacion_redes_luis_espino.pdf. (Consultada el 01/05/2014)

[13] Craig Valli y Murray Brand. (2008). The Malware Analysis Body of Knowledge (MABOK). Obtenido desde http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.149.4690&rep=rep1&type=pdf. - See more at: http://blog.elixircorp.biz/como-hacer-un-analisis-de-malware-parte-3-end/#sthash.m9xJfr1I.dpuf (Consultada el 17/04/2014)

[14] Existe interconexión entre Gauss y otros malwares como STUXNET DUQU o FLAMER, http://www.welivesecurity.com/la-es/2012/08/16/existe-interconexion-entre-gauss-otros-malware-stuxnet-duqu-flamer/ (Consultada el 29/07/2014)

[15] Flame Takes Malware to a Whole New Level, http://www.digitaltrends.com/computing/flame-takes-malware-to-a-whole-new-level/#!bmlDnl (Consultada el 21/05/2014)

11 BIBLIOGRAFIA GENERAL

- How does advanced malware use the network against you?, http://searchnetworking.techtarget.com/feature/How-does-advanced-malware-use-the-network-against-you (Consultada el 12/04/2013)

- How does advanced malware use the network against you?, http://searchnetworking.techtarget.com/feature/How-does-advanced-malware-use-the-network-against-you (Consultada el 20/05/2013)

- Los ataques cibernéticos avanzados pueden ocurrir cada tres minutos, http://mundocontact.com/los-ataques-ciberneticos-avanzados-pueden-ocurrir-cada-tres-minutos/ (consultada el 12/06/2013)

- Malware, http://www.techterms.com/definition/malware (consultada el 12/07/2013)

- Android app malware rates jump 40 percent, http://www.zdnet.com/android-app-malware-rates-jump-40-percent-7000019093 (consultada el 12/08/2013)

- Sandboxing, http://www.techopedia.com/definition/25266/sandboxing (consultada el 20/08/2013)

- Estudiando a Flame, http://antisec-security.blogspot.com.ar/2013/02/estudiando-flame-modulos-en-este-post.html (Consultada el 09/10/2013)

- Kapersky Lab, http://latam.kaspersky.com/ (Consultada el 06/03/2014)

- It's Time to Open Our Eyes to Advanced Malware Protection, http://www.securityweek.com/its-time-open-our-eyes-advanced-malware-protection. (Consultada el 24/03/2014)

- SKYWIPER (a.k.a Flame a.k.a Flamer), http://www.crysys.hu/skywiper/skywiper.pdf (Consultada el 24/03/2014)

- http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet (Consultada el 15/05/2014)

- Bitacora del analista de Virus, http://www.viruslist.com/sp/weblog?weblogid=208188631 (Consultada el 15/05/2014)

- Amit Malik. (2013). Reversing Basics – A Practical Approach Using IDA Pro. http://securityxploded.com/reversing-basics-ida-pro.php - Top ten de virus, http://www.pcauthority.com.au/News/143993,top-ten-worst-viruses.aspx (Consultada el 21/05/2014)

- Target missed alarms in epic hack of credit card data? http://www.businessweek.com/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data?mkt_tok=3RkMMJWWfF9wsRokv63Le%2B%2FhmjTEU5z16egpXaK%2BgYkz2EFye%2BLIHETpodcMTcRhPbrYDBceEJhqyQJxPr3FLdkNw9Z3RhTiDw%3D%3D#p1 (Consultada el 21/05/2014)

- Win32/Palevo,http://www.symantec.com/security_response/writeup.jsp?docid=2009-072313-3630-99 (Consultada el 18/06/2014)

- Win32/Alureon, http://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?name=Win32%2fAlureon (Consultada el 20/06/2014)

- CVE, https://cve.mitre.org / (Consultada el 18/06/2014)

- Info sobre codificación base64, http://www.base64decode.org/ (Consultada el 20/06/2014)

- http://www.rpp.com.pe/2012-03-06-lulzsec-y-anonymous-conozca-sus-diferencias-noticia_458383.html (Consultada el 20/06/2014)

- Next Generation Firewall , http://www.gartner.com/it-glossary/next-generation-firewalls-ngfws/ (Consultada el 20/06/2014)

- Hacktivist declare war against all organizations, what you can do about it? https://www.brighttalk.com/webcast/7477/49385 (Consultada el 20/06/2014)
- Common Vulnerabilities and Exposures http://searchfinancialsecurity.techtarget.com/definition/Common-Vulnerabilities-and-Exposures (Consultada el 24/06/2014)

- Blended Threats, http://searchsecurity.techtarget.com/definition/blended-threat (Consultada el 24/06/2014)

- https://www.microsoft.com/en-us/windows/enterprise/products-and-technologies/virtualization/operating-system/default.aspx (Consultada el 24/06/2014)

- BYOD http://whatis.techtarget.com/definition/BYOD-bring-your-own-device (Consultada el 24/06/2014)

- MDM, http://searchmobilecomputing.techtarget.com/definition/mobile-device-management, (Consultada el 24/06/2014)

- Defining Cultivating Measuring Enterprise Agility, https://www.gartner.com/doc/491436/defining-cultivating-measuring-enterprise-agility (Consultada el 24/06/2014)

- Cloud-Based Sandbox http://www.sourcefire.com/products/advanced-malware-protection/cloud-based-sandbox. (Consultada el 29/06/2014)

- Server and Cloud Platform, http://www.microsoft.com/en-us/server-cloud/solutions/virtualization.aspx#fbid=7SPNVOcneNq. (Consultada el 29/06/2014)

- VMWARE TOOLS, http://searchservervirtualization.techtarget.com/definition/VMware-Tools. Consultada el 29/06/2014)

12 ANEXOS

12.1 PRUEBAS DE CONCEPTO

El objetivo principal de la prueba de concepto es analizar el comportamiento de los malwares descritos en el capítulo 6 mediante un laboratorio que permita correr estos malwares sobre la topología estudiada de manera controlada. Para ello, se utiliza tecnología de virtualización ESX 5.5 VMWARE de tal forma que permita recrear toda la topología de red y los servicios estudiados a través de la encuesta realizada que brindo información junta el análisis de los diseños de las distintas redes de clientes organizacionales. Posteriormente se realizan pruebas de infección llevando las muestras de malware directamente sobre los equipos a través de protocolos de transmisión conocidos como FTP/CIFS.

Los recursos físicos disponibles por parte del servidor Blade asignados para el montaje de la topología completa junto con los elementos de seguridad.

Recursos	**Cantidad Máx**
Virtual Switches	Ilimitado
Virtual CPUs	16 vCPUs
Memoria RAM	12GB
Espacio en Disco	2TB

Tabla 4. Asignación de recursos

A continuación se describe define la arquitectura montada y los servicios.

- DEFINICION Y ARQUITECTURA DE PLATAFORMAS INVOLUCRADAS ARMADO DE TOPOLOGIA DE RED

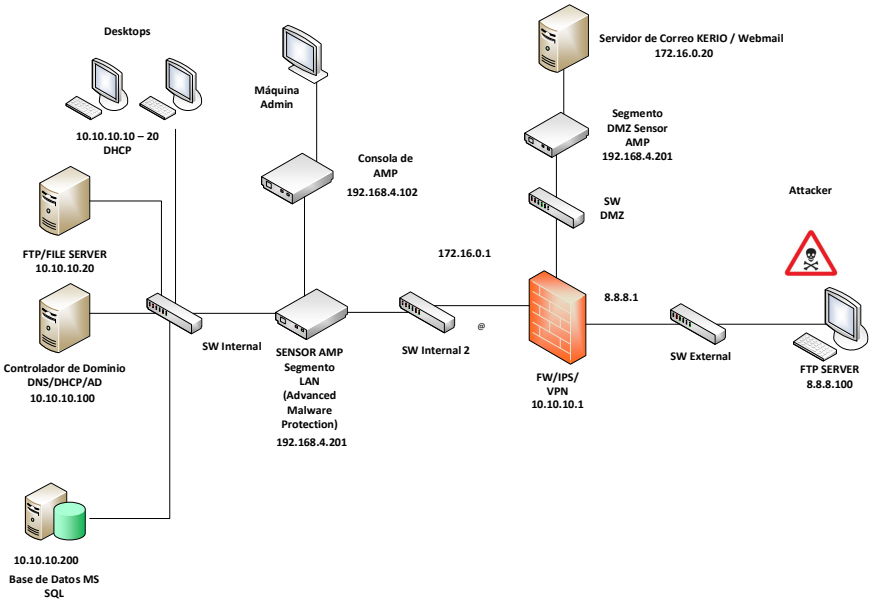


Figura 4. Topología de red diseñada y montada en laboratorio

La topología final de red montada en base a los resultados de la investigación para la prueba de concepto es la ilustrada en la siguiente figura 4. Debido a la variedad de servidores y tecnologías en seguridad para poder montar la arquitectura diseñada, se opta por trabajar para la PoC con tecnología virtualizada VMware ESX v5.5.

VMware es una plataforma de virtualización que permite la recreación de ambientes netamente físicos en ambientes completamente virtuales a partir de la tecnología Hypervisor, optimizando y mejorando los recursos. Una de sus ventajas para esta prueba de concepto es que el producto no se ve limitado a nivel de licenciamiento para la puesta en producción del laboratorio.

Paralelamente se utilizan herramientas propias del fabricante (ej: VMwaretools) para optimizar los recursos para el laboratorio, esta herramienta permite mejorar y complementar el mejor desempeño del ambiente virtual y si asegurar el performance

de cada máquina virtual en el montaje de la topología seleccionada. Se tuvo en cuenta la relación que existe directamente entre el consumo de cada servicio y el posible comportamiento de los ataques a simular ya que la mayoría de los encuestados confirma que los mayores ataques recibidos en sus empresas están relacionados con virus, troyanos entre otros los cuales afectan y utilizan el comportamiento de cierto servicio para fines propios.

En totalidad para la simulación de los servicios y la topología se utilizaran 10 máquinas virtuales y otras dos máquinas para fines netamente administrativos. La Figura 5 ilustra la consola de administración.

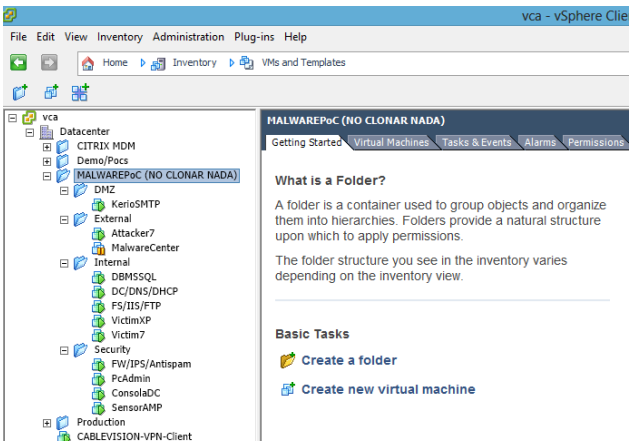


Figura 5. Consola de administración VWMARE ESX

A continuación se listan los siguientes servidores y plataformas de seguridad:

Servidores DMZ

Servidor Correo **(KerioSMTP)**

Red Interna

Servidor Base de datos **(DBMSSQL)**

Servidor controlador de Dominio y servicios de Directorio **(DC/DNSS/DHCP)**

Servidor de Archivos compartidos y transferencia de archivos **(FS/ISS/FTP)**

Cliente Victima 1 **(VictimaXP)**

Cliente Victima 2 **(Victima7)**

Red Externa

Atacante **(Attack7)**

Servidor de Malware **(MalwareCenter)**

SEGURIDAD PERIMETRAL

Primera Generación

Firewall, Filtrado Web, IPS,AntiSpam **(FW/IPS/AntiSpam)**

Próxima Generación

Sensor de Malware avanzado **(SensorAMP)**

Consola del sensor **(ConsolaDC)**

Nombre Máquina	Red	Servicios	Descripción
KerioSMTP	DMZ	SMTP Correo, Webmail (HTTPS)	Servicios de Correo
DC/DNS/DHCP	Interna	DNS, Active Directory, DHCP	Servicios de Controlador de Dominio
DBMSSQL	Interna	SQL	Servicios de Base de datos
FS/ISS/FTP	Interna	FTP, HTTP, CIFS	Servidor de File Server
Victim7	Interna	NA	No aplica
VictimXP	Interna	NA	No aplica
Attacker7	Externa	NA	No aplica
MalwareCenter	Externa	NA	No aplica
ConsolaDC	Seguridad	HTTPS	Consola
SensorAMP	Seguridad	NA	No aplica
FW/IPS/AntiSpam	Seguridad	Navegación (HTTP, HTTPS, FTP)	Navegación/Publicación

Tabla 5. Máquinas, servidores, servicios y seguridad.

Los recursos del ambiente a utilizar asignados respectivamente a cada máquina virtual:

Máquinas Virtuales	GB	HD	vCPU
Exchange2003	1	40	1
BD_Server	1	40	1
DC2003+DHCP	1	40	1
FS+FTP	1	40	1
VictimaXP	1	20	1
Attack7	1	20	1
FW_IPS_1	1	20	1
Sensor 3D	2	100	2
VirtualDC64	2	40	4

Tabla 6. Asignación de recursos

La VirtualDC64 encargada de analizar el malware cuenta con más ciclos de CPU para el análisis debido a que debe procesar los logs de tráfico enviados desde el sensor.

- **SERVICIOS VIRTUALIZADOS**

Servidor Exchange Kerio Connect (SMTP / Webmail) 172.16.10.20

Se seleccionó la plataforma Kerio Connect debido a dos factores: El producto es una versión light de los servicios de Exchange de la plataforma Windows, esta opción permite montar el servidor de SMTP sin complejidad y sin alto consumo de recursos, la segunda es que brinda licencia demo de 30 días para la prueba del producto. Este servidor cuenta con los usuarios del dominio integrados para realizar las pruebas así se podrá visualizar la cuenta de los usuarios como Alex Turner para un posterior análisis.

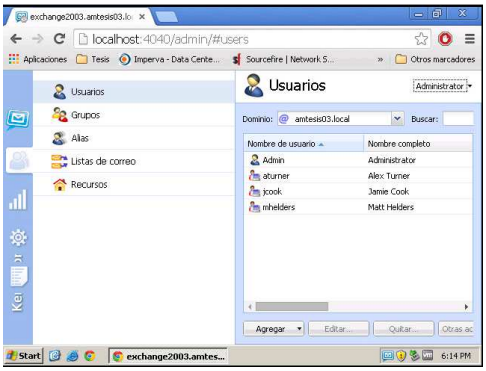


Figura 6. Consola de administración KERIO CONNECT

Los servicios listados dentro de la administración del producto se pueden visualizar en el tab de servicios como muestra la figura 7.

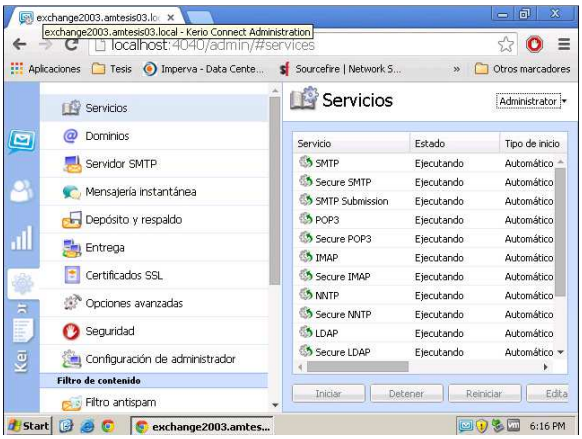


Figura 7. Consola de Servicios activos en KERIO CONNECT

Servicios de Dominio, DNS y DHCP servicios en servidor de 10.10.10.100

Dentro del servidor DC/DNS/DHCP se encuentran instalada la base de usuario de pruebas y los servicios de DC, DHCP y DNS. Las máquinas de la red interna podrán obtener una dirección IP asignada de manera automática y se utilizaran los mismos usuarios integrados al correo para la autenticación

Obviamente los servicios de y autenticación por Kerberos o NTLM se encuentran también disponibles.

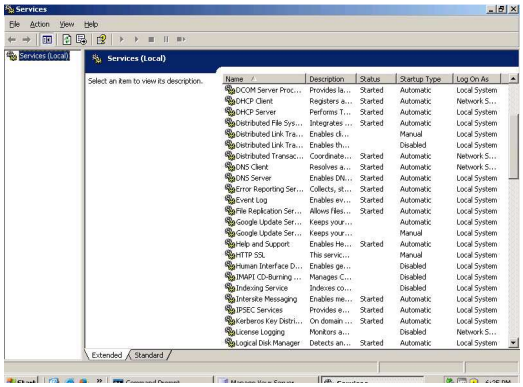


Figura 8. Consola de servicios WINSERVER

SERVIDOR DE BASE DE DATOS SQL 10.10.10.102

Los servicios de base de datos MSSQL Server 2003 encuentran activos e instalados y son gestionados a través de la consola del *SQL Server Configuration Manager* y para la creación de instancias de la base de datos como se ilustran en las figuras 9 y 10, 11.

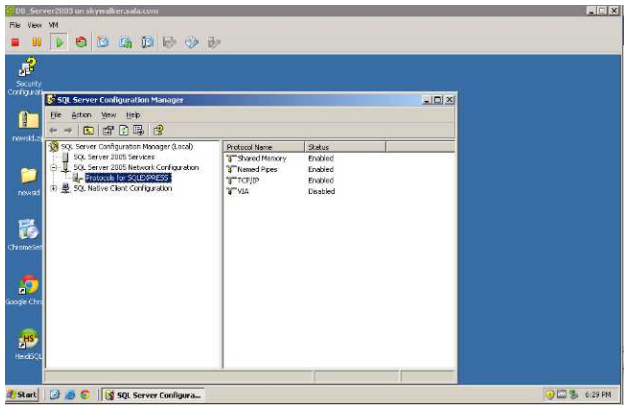


Figura 9. Consola SQL Server Configuration

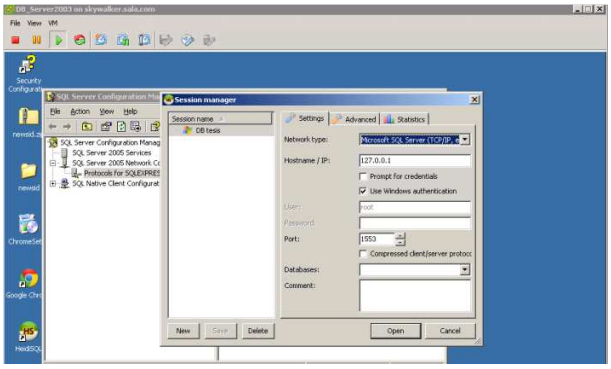


Figura 10. Consola SQL Server Configuration

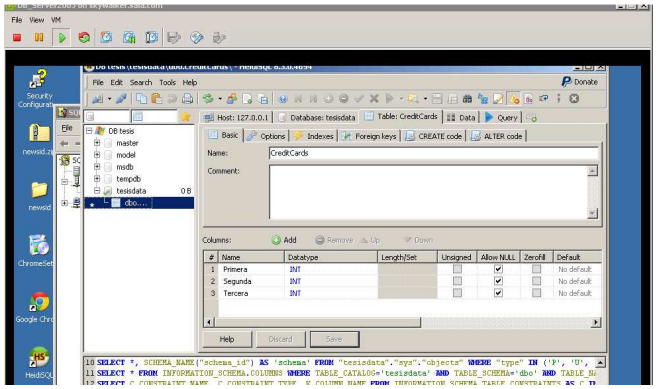


Figura 11. Instancia de base de datos creada

FileServer y IIS (SERVIDOR DE APLICACIONES) 10.10.10.22

Los servicios activos dentro del servidor de File Server los cuales el módulo de File Server de Windows, Filezilla FTP y el motor Web de IIS 6.0 para el desarrollo Web se encuentran iniciados y corriendo en el servidor de File Server como ilustra la figura 13.

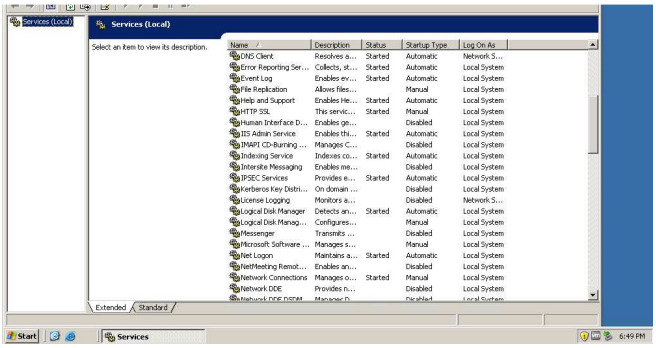


Figura 12. Servicios de File Server e IIS

POLITICAS DE FIREWALL E IPS 10.10.10.1

Las políticas de Firewall e IPS están configuradas para permitir la navegación de los usuarios y servicios hacia internet como HTTP, HTTPS, DNS entre otros Desde la red externa solo existen servicios de publicación para el correo y el Webmail de la plataforma Kerio Connect que se encuentra en la DMZ, en la figura 13 se ilustran la política con sus respectivas reglas.

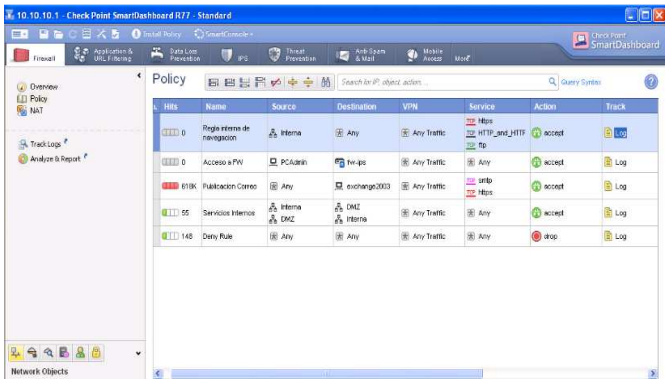


Figura 13. . Consola de administración FW Checkpoint

El IPS analiza el tráfico entrante y saliente a través del módulo Firewall, no se encuentra realizando ningún bloqueo y solo monitorea el tráfico.

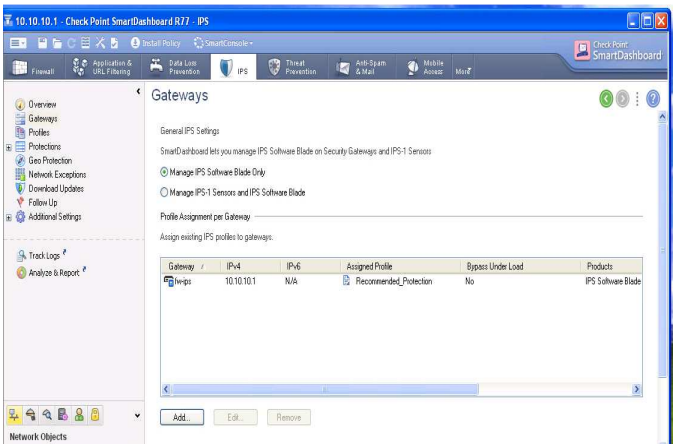


Figura 14. Consola de administración IPS Checkpoint

- CONSOLA DE AMP Y MODULO DE MALWARE AVANZADO

La consola de Advanced Malware Protection cuenta con una configuración inicial de políticas solamente de monitoreo para el tráfico en la red. No obstante este módulo tiene acceso a internet para los ***Malware Cloud Lookups*** que realiza el módulo para la detección de archivos sospechosos.

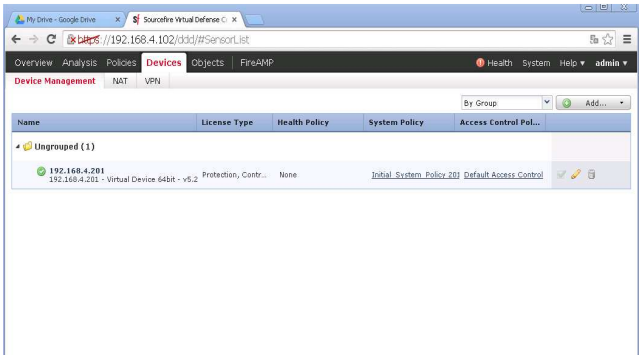


Figura 15. Consola de administración sensor AMP

Las políticas de acceso creadas para permitir el tráfico, inspeccionarlo y loguearlo con el sensor de malware se ilustran en la figura 16.

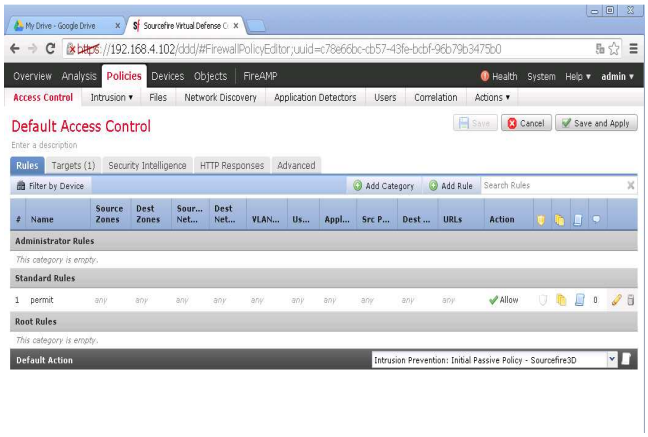


Figura 16. Consola de administración AC

La figura 17 ilustra las políticas de monitoreo y detección para análisis de archivos en la nube y detección, por último se realiza una configuración de parámetros para que la detección de archivos y malware para el afinamiento de detección como se ilustra en la figura 18.

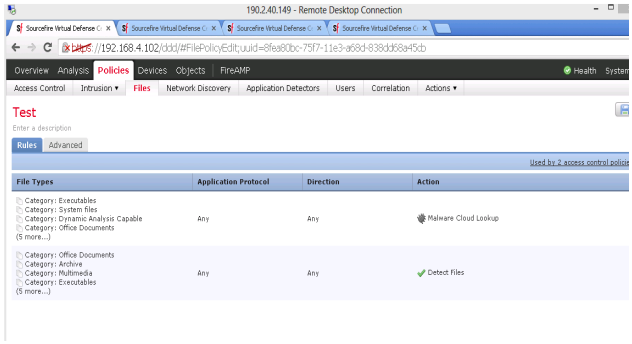


Figura 17. Políticas de monitoreo y transferencia de archivos

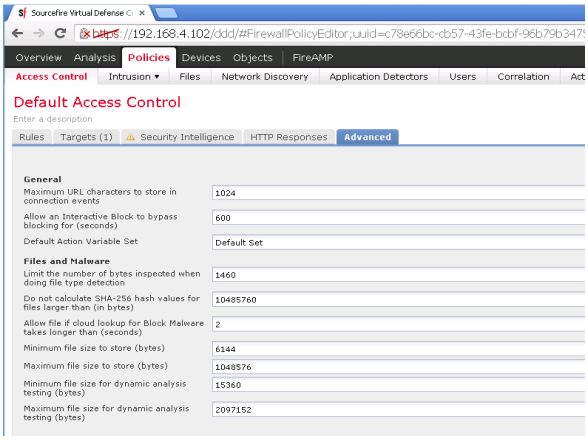


Figura 18. Parámetros de detección para archivos y malware

Es importante remarcar que se hicieron muchas configuraciones adicionales que no son descritas en el presente anexo para la plataforma virtual y lograr la integración de la tecnología en el ambiente.

- **INICIO PRUEBAS DE CONCEPTO**

Para iniciar la prueba de concepto luego todo el montaje virtual inicialmente se realiza una infección trayendo archivos desde la maquina atacante 8.8.8.100 a través de su servicio FTP server realizando una desde las maquinas victimas **(*VictimXP y Victim7*).** Se utiliza el usuario ***"Alex Turner" y "Matt Helders"*** para la inyección de código malicioso dentro de las maquinas como ilustra la figura 19.

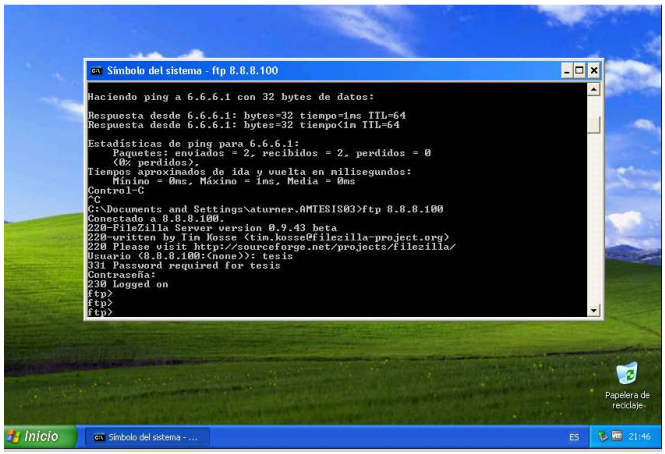


Figura 19. CMD Máquina victima 1

Nota: Se descarga el malware sobre las maquinas con permisos de usuarios de lectura solamente no a nivel de configuración en las máquinas de prueba, las figuras 21 y 22 ilustran el proceso de transferencia a través del protocolo FTP.

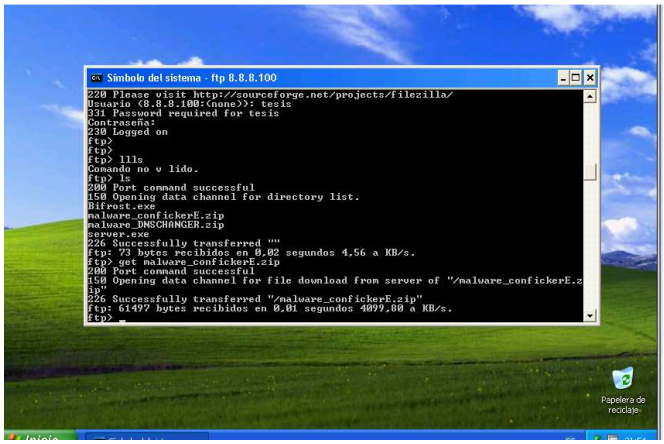


Figura 20. Transferencia Máquina victima 1

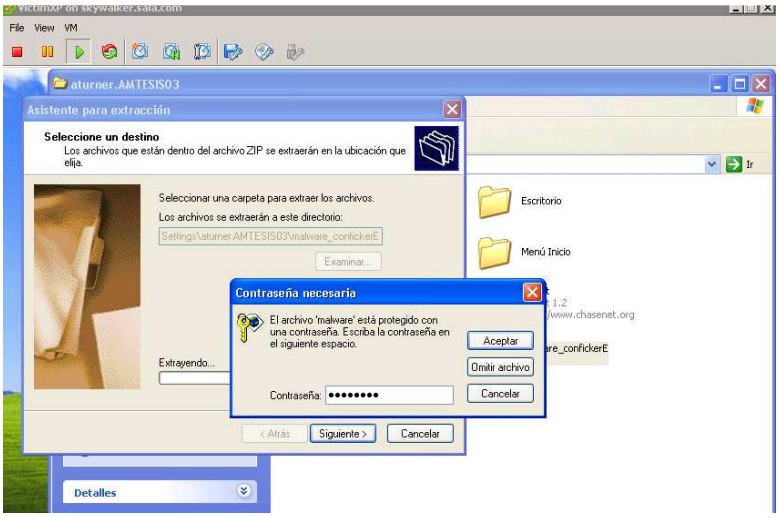


Figura 21. Descompresión malware

Una vez descargado el malware en la maquina victima 1 se infecta la maquina utilizando el password para descomprimir el archivo .zip que contiene la muestra de malware como ilustra la figura 21.

Se procede igualmente con la infeccion de maquinas para otro usuario en este caso ***"Matt Helders"*** mhelders en la maquina Victim7 como ilustra la figura 22

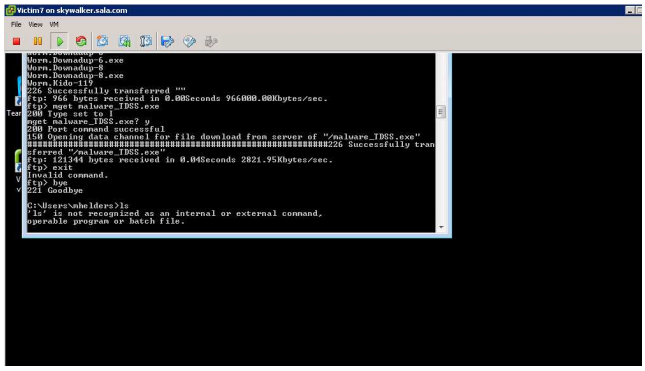


Figura 22. Máquina victima 2

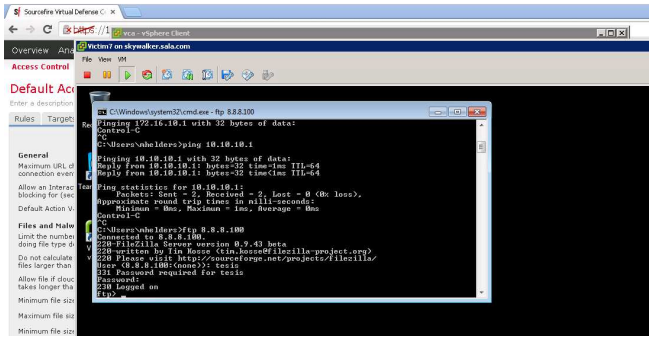


Figura 23. Transmisión malware Máquina victima 2

Se transmite el archivo al destino a través del protocolo FTP Figura 22.

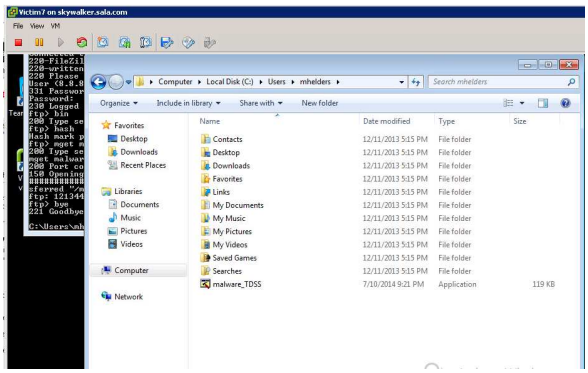


Figura 24. Código malware Máquina victima 2

Y una vez se puede visualizar la muestra de malware como en la figura 23, se procede a ejecutar el código directamente del archivo de malware transmitido como ilustra la figura 24.

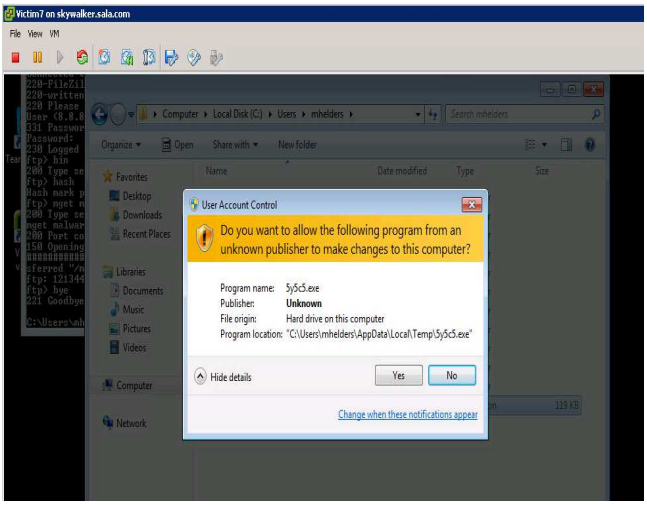


Figura 25. UAC Máquina victima 2

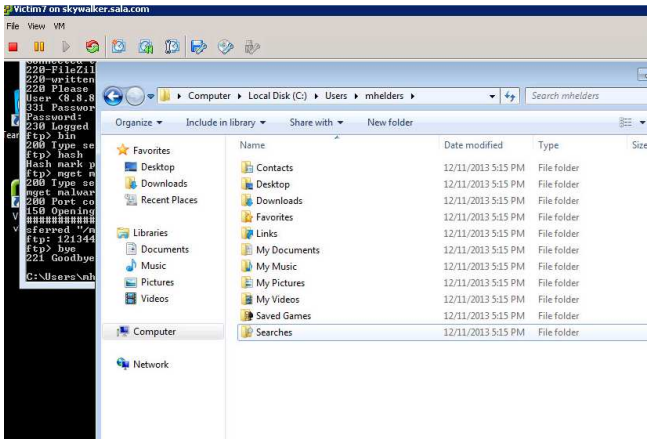


Figura 26. Malware no listado Máquina victima 2

Una vez se corre el ejecutable de la muestra de malware, el archivo original desaparece del directorio figura 25.

Una vez se repliega dentro de la maquinas se monitorea el tráfico de red en el entorno durante un tiempo el estado de los servicios y el comportamiento de la red a través de la consola de administración del producto que analiza todo los logs de tráfico y eventos de detección en las máquinas de la red. La idea principal es dejar que las muestras utilizadas de malware tengan su comportamiento para posteriormente monitorear este desde la consola de administración.

- **ANALISIS DE MALWARE EN LA RED**

Para poder realizar este tipo de análisis, es necesario contar con tecnología que albergue todos los eventos del trafico analizado durante las infecciones de malware en la red (figura 26), como principalmente el análisis no es sobre los servidores, maquinas finales o servicios de estos se realiza un análisis general de toda la red utilizando la consola de administración en base a las infecciones realizadas.

Figura 27. Consola de administración AMP

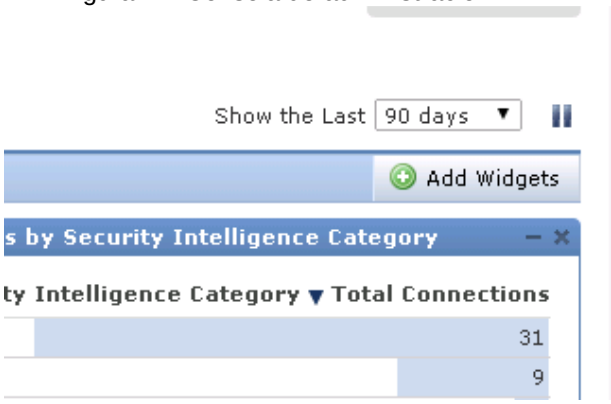


Figura 28. Logs de 3 meses aproximadamente

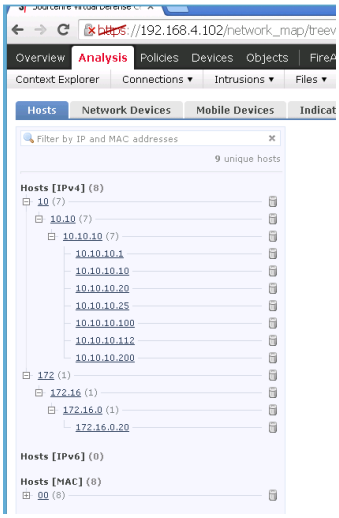


Figura 29. Contexto de red de la topología

Como primer paso se amplía el espectro de tiempo para los eventos de tráfico registrados los últimos 3 meses por la consola, el inicio de la infección fue desde el mes de Abril (Abril, Mayo, Junio) utilizando la opción que se ilustra en la figura 26 Con la tecnología para la detección (context awareness) se realiza un estudio los servidores y maquinas detectadas por la plataforma actual conectadas en los diferente segmentos de red como se ilustran en la figura 27

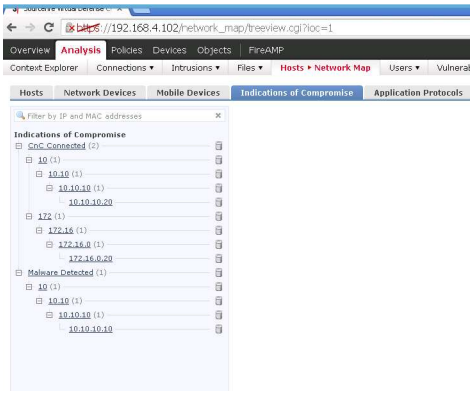


Figura 30. Maquinas infectadas y comprometidas.

En la figura 28 se listan las infecciones de malware y conexiones tipo CnC dentro del ambiente de pruebas.

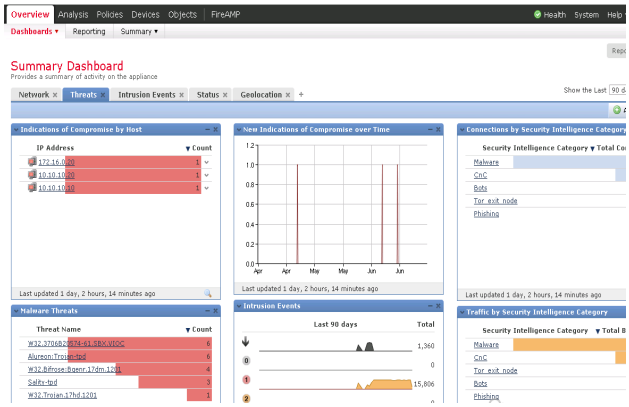


Figura 31. Maquinas infectadas y comprometidas

En la figura 29 se detallan las maquinas infectadas de malware y los focos de infección que se encuentran en las maquinas, las cuales son:

172.16.0.10 Servidor Kerio Connect Correo

10.10.10.20 File Server

10.10.10.10 Windows Victim1

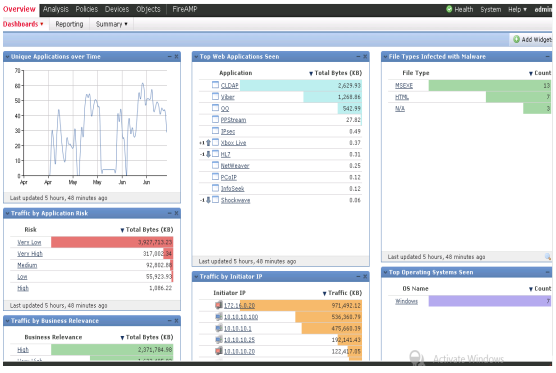


Figura 32. Resumen de tráfico de análisis

La figuras 30 y 31 ilustran el trafico detectado en correlación a las maquinas infectadas.

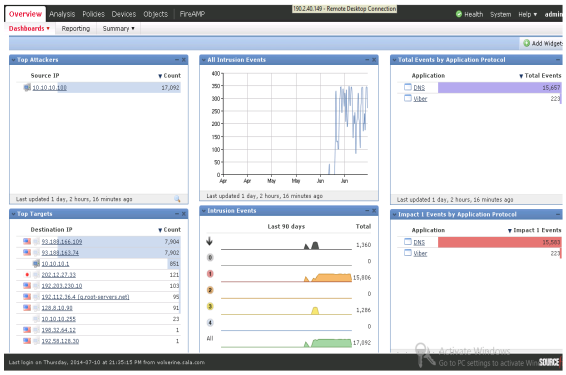


Figura 33. Segundo resumen de tráfico de análisis

En el análisis de conexiones se puede notar que existen intentos de conexión hacia dominios externos por medio del protocolo DNS, estos intentos son detectados con eventos de intrusión desde la maquina 10.10.10.100 Servidor de Active Directory y se ilustra en la figura 32.

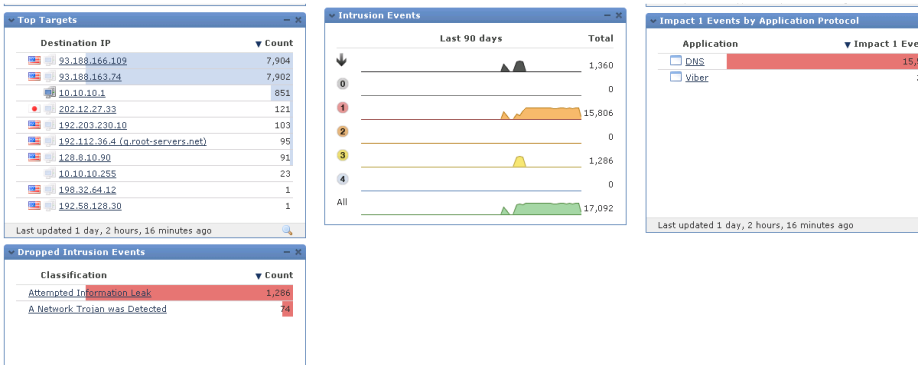


Figura 34. Solicitudes DNS por parte de máquinas infectadas

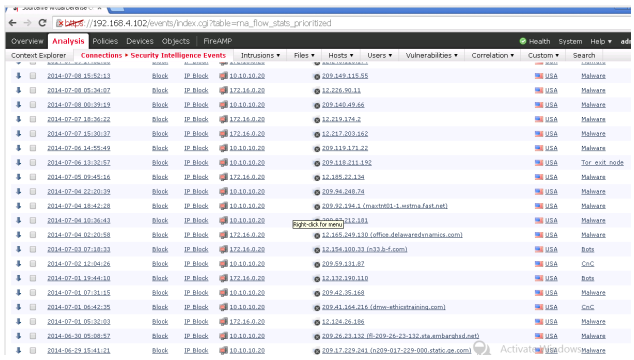


Figura 35. Log de conexiones desde maquinas comprometidas

Realizando un despliegue como se ilustra en la figura 33 se pueden ver se pueden visualizar intentos de conexión desde la maquina 10.10.10.20 y la maquina 172.16.0.10 los cuales registran eventos asociados a Malware, conexiones CnC y eventos de phising desde el servidor de correo.

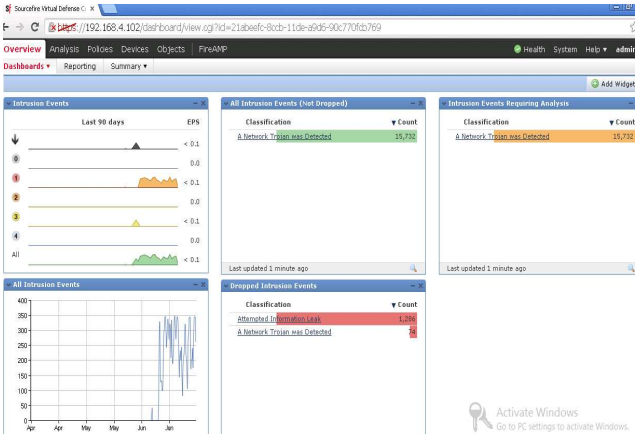


Figura 36. Log de conexiones desde maquinas comprometidas

Existen registros de tráfico que está correlacionados a eventos de intrusión, estos han sido detectados a partir del servidor de dominio el cual tiene una variante troyana de red detectada como se ilustra en el 5 widget de la figura 34.

- **Análisis de malware variante WIN32/Alureon.**

A continuación se realizara un análisis de cada infección encontrada en la red luego de realizar un análisis general del estado de las máquinas y tráfico en la red. Inicialmente se puede notar que existen tres máquinas en total infectadas y con comportamientos anómalos detectados por la herramienta como se ilustra en la figura 35.

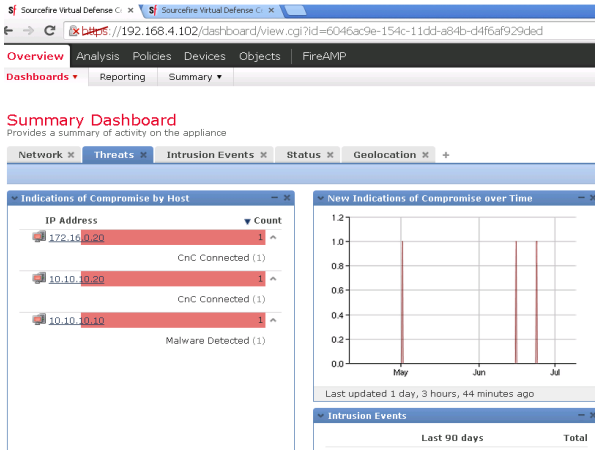


Figura 37. Maquinas comprometidas

Para conocer las propiedades de infección de cada máquina se revisa el perfil de host creado por la herramienta al momento de ser reportado por el sensor como se ilustra en la figura 36

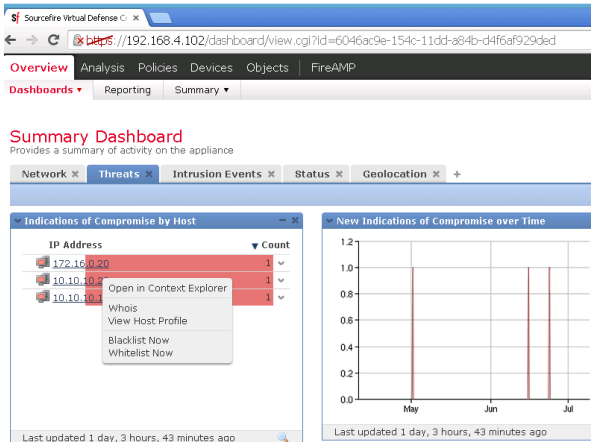


Figura 38. Características de hosts comprometidos

Una vez se accede al perfil del host, en este caso al servidor de correo 172.16.0.20 se puede ilustrar como muestra la figura 37 las distintas características del servidor como su dirección IP asignada, MAC, y servicios locales activos. Para este servidor el malware trata de crear una conexión CnC desde el mismo servidor, estos intentos son visualizados en la figura 38.

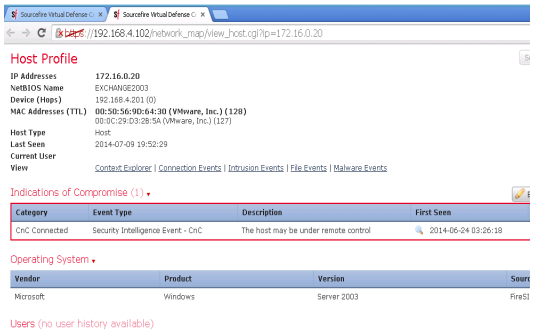


Figura 39. Detección de conexiones CnC

Otro tipo de intentos de conexiones hacia servidores externos detectados por la herramienta son conexiones tipo TOR EXIT NODE que son conexiones cifradas o conexiones tipo Bot automáticas e intento de trafico phising hacia servidores servidores externos como se ilustran 38, 39 y 40.

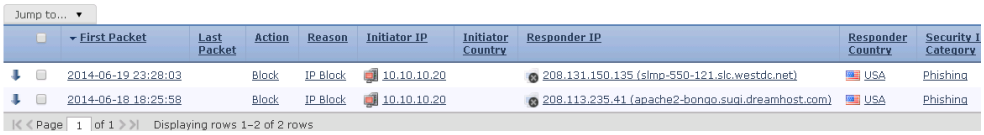


Figura 40. Intentos de conexión tipo CnC desde el servidor de correo

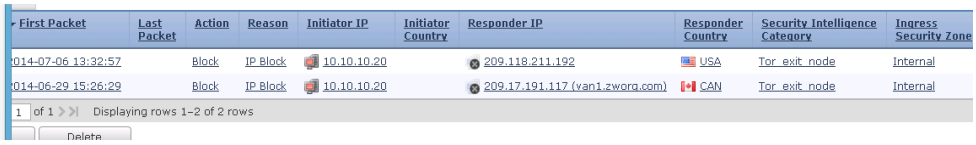


Figura 41. Intentos de conexión tipo Tor Exit Node

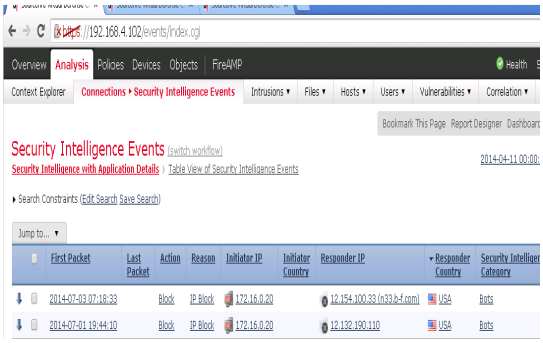


Figura 42. Conexión tipo Bots

Figura 43. Intentos de conexión tipo Tor Exit Node

Realizando una análisis más detallado sobre otra máquina infectada se puede notar que el malware fue detectado en la maquina debido a la transferencia del malware en la maquina como se ilustra en su perfil detallado en las figuras 42 y 43

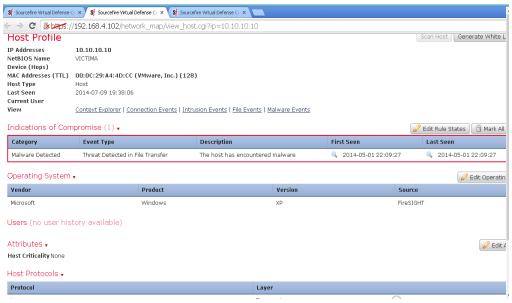


Figura 44. Malware detectado por la transferencia de archivo

Figura 45. Malware detectado en maquina victima

La variante detectada en el análisis anterior en las maquinas infectadas está asociada al comportamiento del malware Alureon utilizada para realizar el análisis de comportamiento en la red, una de sus principales características fueron descritas

al tratar de establecer conexiones por diferentes tipos de métodos como los mencionados anteriormente

- **Análisis de malware variante WIN32/Palevo.**

A continuación se realiza un estudio sobre el comportamiento de las firmas disparadas por el tráfico visto y asociado a las conexiones desde el servidor Active Directory, para ello se analiza el perfil del servidor como se ilustra en la figura 44. Desde el servidor se está tratando de realizar un portscan automatizado al firewall Gateway para conocer que puertos están abiertos, ya que las firmas que se dispararon están asociadas a este tipo de escaneos.

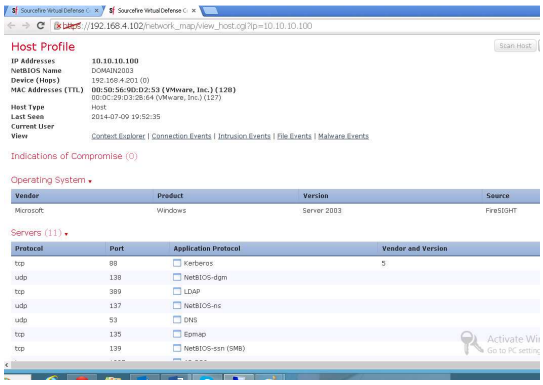


Figura 46. Perfil de servidor de correo

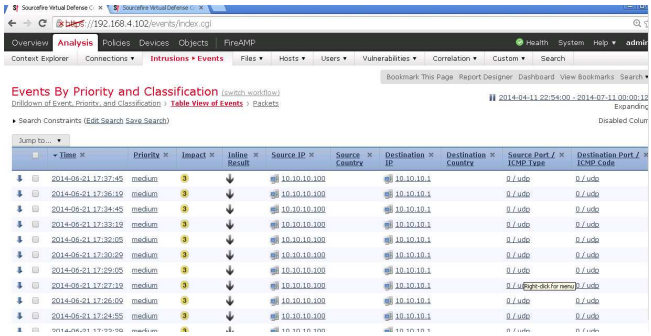


Figura 47. Firmas detectadas asociadas al tráfico del servidor

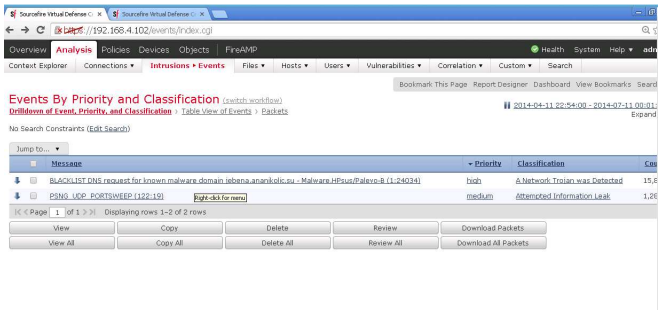


Figura 48. Firmas detectadas asociadas a la variante de Palevo

La variante de Palevo asociada al tráfico que dispara las firmas del sensor de SNORT es HPSUS/Palevo-B como se ilustra en la figura 46, no solamente utiliza realiza este tipo de ataques sino también realiza consultas de Black DNS como se ilustra en la figura 47 a dominios como:

- jebena.ananikolic.su
- peer.pickeklosarske.ru
- teske.pornicarke.com

.

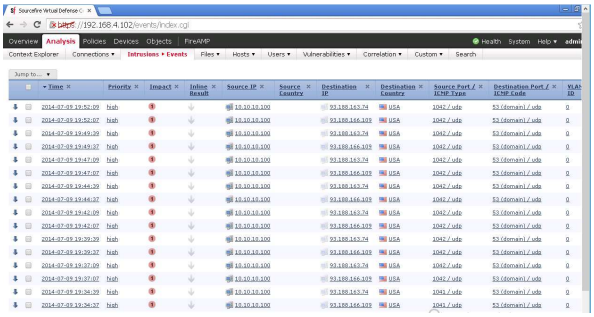


Figura 49. Firmas detectadas asociadas a la variante de Palevo

- ANALISIS DE TRAFICO MALICIOSO GENERADO EN LA RED

Para la prueba de concepto, no fue generado ningún tipo de tráfico en especial, ni tampoco existe conexión alguna hacia internet por parte de las maquinas montadas en el laboratorio, a continuación se puede ver que debido a las conexiones que tratan de realizar los malwares previamente analizados y el comportamiento de este en la red se visualiza tráfico hacia redes externas debido a

las múltiples solicitudes de conexión que tratan de realizar y son detectadas por el sensor de malware como se ilustra en la figura 47.

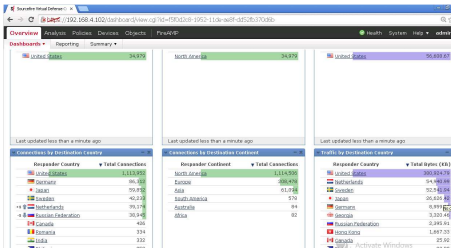


Figura 50. Dashboard de consulta a servidores externos

La figura 48 ilustra el espectro en el tiempo de cómo fue trasmitido desde la maquina atacante a través del protocolo FTP transferencia de archivos que fueron catalogados por el análisis del sensor de red como malware, los hash de las muestras de malware pueden ser diferentes debido a que las muestras del malware original pueden tener ciertas limitantes a nivel de comportamiento que el malware original desarrollado

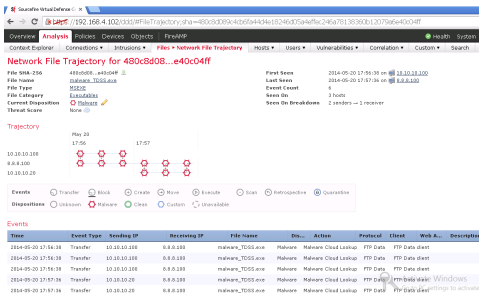


Figura 51. Espectro de malware transmitido desde 8.8.8.100

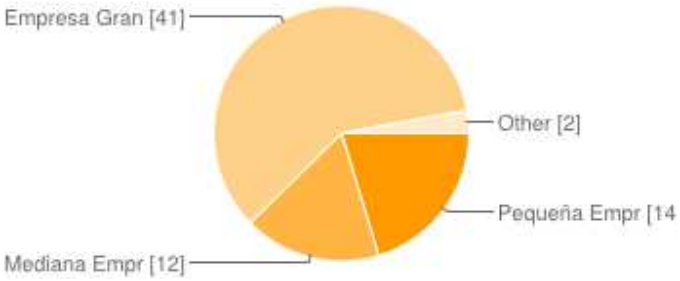
12.2 ENCUESTA Y RESULTADOS

La siguiente encuesta fue realizada regionalmente a personal relacionado al área de IT y Seguridad como consultores, ingenieros, coordinadores, etc. Para conocer en detalle las organizaciones actualmente, también se presentan los resultados estadísticos de la misma encuesta que soportaron los estudios y pruebas de concepto realizadas.

Por favor seleccione su país

Argentina	32	46%
Bolivia	0	0%
Chile	1	1%
Colombia	29	42%
Ecuador	1	1%
Paraguay	5	7%
Perú	0	0%
Uruguay	0	0%
Venezuela	1	1%
	0	0%

1- ¿En qué tipo de empresa trabaja actualmente?

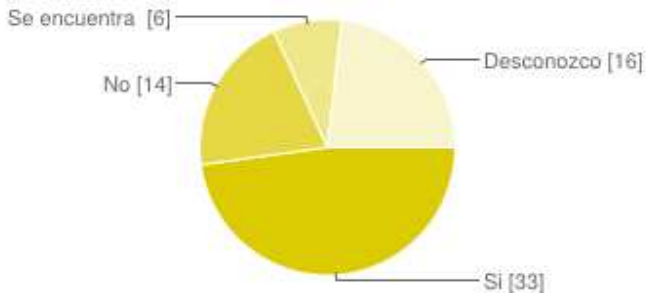


Pequeña Empresa (de 10 hasta 50 empleados)	14	20%
Mediana Empresa (de 50 hasta 200 empleados)	12	17%
Empresa Grande (más de 200 empleados)	41	59%
Other	2	3%

2- Por favor seleccione en que sector se desarrolla la empresa donde trabaja

Bancaria / Financiera	8	12%
Gubernamental	4	6%
Educacional	2	3%
Servicios Básicos/Generales/Corporativos	11	16%
Salud	2	3%
Sin ánimo de lucro	0	0%
Retail	2	3%
HW/SW/Tecnología	9	13%
Comunicaciones	9	13%
Other	22	32%

3- ¿Existe algún BCP o plan de contingencia dentro de su empresa?

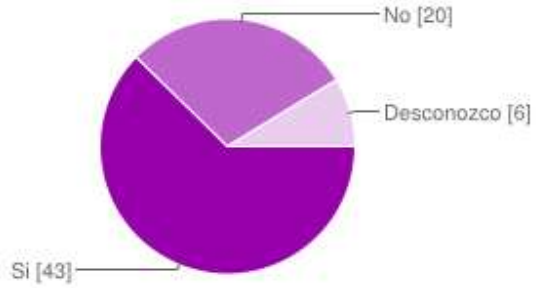


Si	33	48%
No	14	20%
Se encuentra en desarrollo	6	9%
Desconozco	16	23%

4- ¿En qué área tecnológica se desempeña dentro de su empresa?

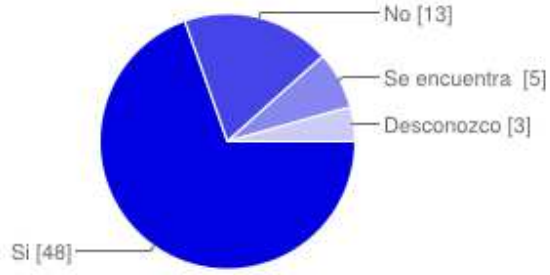
Infraestructura (IT Networking)	18	26%
Servidores y aplicaciones	6	9%
Desarrollo	6	9%
Seguridad Informática	14	20%
Consultoría/Auditoria	10	14%
Proyectos/Coordinación	8	12%
Other	7	10%

5- ¿Actualmente la empresa donde trabaja cuenta con área de seguridad informática?



Si	43	62%
No	20	29%
Desconozco	6	9%

6- ¿Existen políticas de seguridad establecidas actualmente en su empresa?

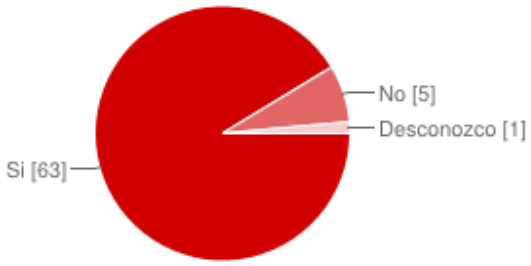


Si	48	70%
No	13	19%
Se encuentra en desarrollo	5	7%
Desconozco	3	4%

7- Seleccione en que tecnología(s) está basada y soportada la infraestructura tecnológica dentro de su empresa

Hardware/Software propietario	40	39%
Hosting/Housing/SaaS	11	11%
Ambiente Virtualizado	20	20%
Todas (Híbrida)	31	30%

8- ¿La infraestructura tecnológica de su empresa permite conexiones Inalámbricas (Wireless) para las áreas de trabajo y acceso a internet?



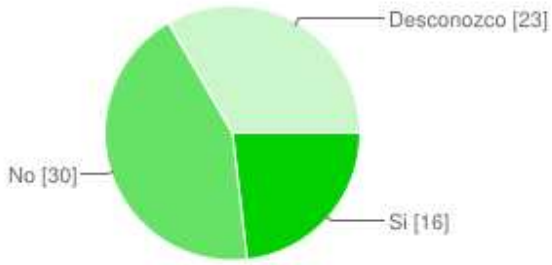
Si	63	91%
No	5	7%
Desconozco	1	1%

9 - Indique que tipos de soluciones perimetrales refuerzan la seguridad de su empresa actualmente

AntiSpam	43	16%
Firewall/UTM	58	22%
Antivirus	57	21%
IPS	29	11%
DLP	9	3%

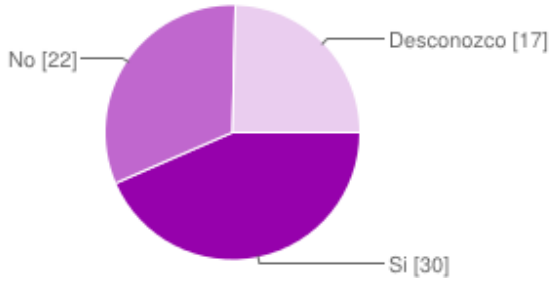
WAF (Web Application Firewall)	15	6%
Proxy/Filtrado Web	51	19%
Desconozco alguna	4	1%
Other	2	1%

10- ¿Su empresa cuenta con servicios a nivel de hosting/housing/SaaS contratados a nivel de seguridad?



Si	16	23%
No	30	43%
Desconozco	23	33%

11- ¿Su empresa cumple con normativas de seguridad a nivel de compliance de acuerdo al sector donde trabaja?

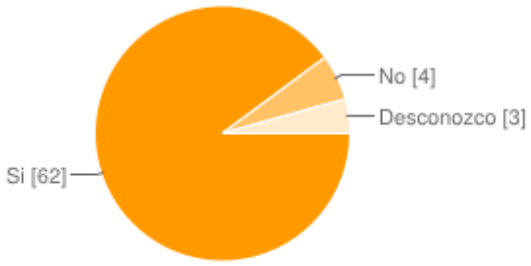


Si	30	43%
No	22	32%
Desconozco	17	25%

12- Por favor seleccione que servicios a nivel de networking y seguridad se brindan en su empresa

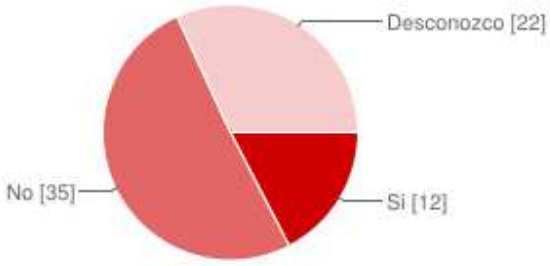
Correo (SMTP/POP3/Webmail)	57	16%
Transferencia de Archivos (FTP,SCP,TFTP)	46	13%
Servicios de Directorio (DC, LDAP,DHCP,DNS)	45	13%
Conexión Remota (VPN, RDP,ICA)	57	16%
Servicios de Autenticación (TACACS+, Radius,Tokens, Firma Digitales)	26	7%
Navegación Internet/Intranet (HTTP/HTTPS)	55	16%
Servidor de Archivos/BD (SQL/NFS/SAMBA)	44	13%
Servicios de Escritorio Virtual (VDI)	21	6%
Other	1	0%

13- ¿Existen aplicaciones web propias desarrolladas por la empresa o aplicaciones desarrolladas por terceros?



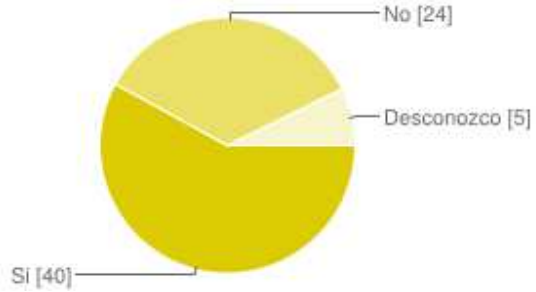
Si	62	90%
No	4	6%
Desconozco	3	4%

14- ¿Su empresa cuenta con certificaciones en seguridad para sus procesos internos y externos?



Si	12	17%
No	35	51%
Desconozco	22	32%

15- ¿Actualmente su empresa permite conexiones de dispositivos móviles y tablets para las aplicaciones web internas o publicadas?

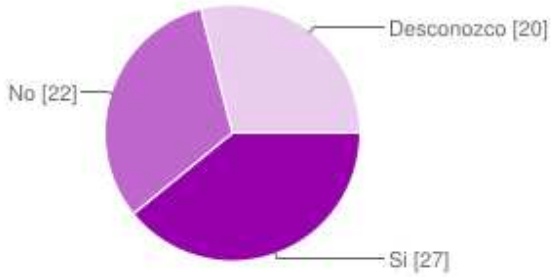


Si	40	58%
No	24	35%
Desconozco	5	7%

16- Por favor seleccione que redes sociales son permitidas comúnmente para los usuarios dentro de su empresa:

Twitter	15	10%
Facebook	14	10%
Linkedin	21	15%
Google+	18	13%
Youtube	13	9%
Flickr	5	3%
Skype	30	21%
Todas (Sin restricción)	27	19%

17- ¿En su empresa han existido incidentes o ataques a nivel de seguridad?

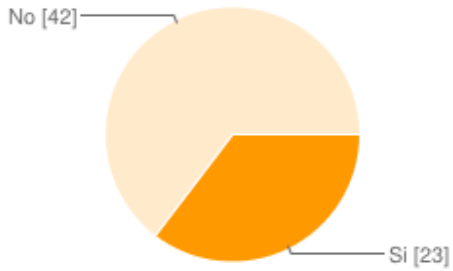


Si	27	39%
No	22	32%
Desconozco	20	29%

18- En caso tal de responder afirmativamente a la pregunta anterior, por favor indique ante qué tipo de ataque o ataques

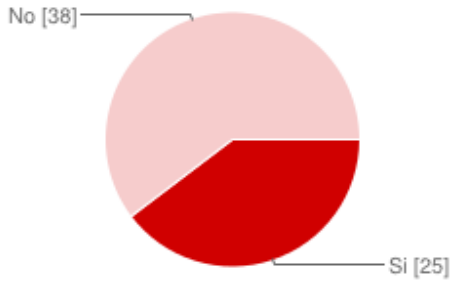
Virus/Troyanos	20	29%
Vulnerabilidad App/OS	8	12%
Malware	17	25%
Denegación de servicio (DoS)	8	12%
Robo de información sensible o intelectual	3	4%
Ataque día cero (Zero Day)	0	0%
Robo de contraseñas, ataques de fuerza bruta	3	4%
Ninguno	7	10%
Other	2	3%

19- ¿Conoce usted si su empresa trabaja con herramientas tipo SIEM?



Si	23	35%
No	42	65%

20- ¿Conoce usted si su empresa se encuentra actualmente protegida ante ataques de malware avanzado?



Si	25	40%
No	38	60%