UNIVERSIDAD DE GUANAJUATO

Nombre: Jorge Omar Martínez López

Asesor: Francisco Javier Velázquez Sagahón

Modalidad: Ejercicio Profesional

ADMINISTRACIÓN, SEGUIMIENTO Y CONTROL DE LA SOLUCIÓN DE ANTIVIRUS "ENDPOINT" DE LA UNIVERSIDAD DE GUANAJUATO.

4. ANTIVIRUS

5. ESTRATEGIAS DE SEGURIDAD EN LA UG

Índice de figuras y tablas

INTRODUCCIÓN

Los avances en las tecnologías de la información, han sido de suma importancia para el progreso de la sociedad. El termino de tecnologías de información comprende las diferentes formas para crear, intercambiar, almacenar, manejar y manipular el material digital.

A medida que vamos utilizando las tecnologías de la información como apoyo para la realización de nuestras actividades de la vida diaria, tanto para las cuestiones personales como de trabajo; sin saber vamos cediendo gran parte de nuestra información personal, ya sea para que sea almacenada por alguna aplicación en nuestro equipo de cómputo o en alguna plataforma administrada por algún tercero. Por desconocimiento del proceso técnico confiamos en que nuestra información se encuentra segura y damos por hecho que no es importante y por ende no le prestamos la atención suficiente a las cuestiones de seguridad.

Los cibercriminales (Hackers de sombrero negro) crean malware que en conjunto con técnicas cada vez elaboradas pueden llegar a tener acceso no autorizado a nuestros equipos sin nuestro consentimiento o sin que nos percatemos de ello, y además pueden llegar a obtener acceso a nuestra información personal o pueden tener la capacidad de controlar nuestros equipos de manera remota para realizar actividades con fines Maliciosos, ya sea para poder obtener algún beneficio monetario o para realizar un ataque informático. Cada vez nos enfrentamos a malware más sofisticado que utiliza nuevas técnicas buscar alguna vulnerabilidad que facilite obtener acceso a nuestra valiosa información; la seguridad convencional ya no es suficiente para mantener nuestros datos e identidad a salvo.

Muchas personas no conocen los riesgos a los que se enfrentan con tan solo navegar en internet ya sea desde su dispositivo móvil o desde su pc sin que cuente con las últimas actualizaciones instaladas.

La Universidad de Guanajuato cuenta con una Coordinación de Seguridad y Monitoreo que depende de la Dirección de Servicios y Tecnologías de la Información, que se encarga de implementar controles, medidas y soluciones basados en estándares internacionales, que ayudan a que la comunidad universitaria pueda hacer uso del servicio de internet con el menor riesgo posible y que el mismo servicio sea óptimo.

Se me dio la oportunidad de poder laborar en dicha Coordinación como el administrador de la solución de antivirus empresarial Institucional, para implementar medidas, controles y estrategias, y así poder manejar de manera adecuada los incidentes de malware y los diferentes ataques relacionados con la seguridad informática que podrían poner en riesgo la información, los servicios y la reputación de nuestra máxima casa de estudios de manera eficiente y transparente para el usuario. En el desarrollo de este trabajo explicare de manera detallada mis actividades

1. UNIVERSIDAD DE GUANAJUATO

1.1. Universidad de Guanajuato

Es una institución de vanguardia cimentada en una tradición de más de dos siglos y medio de vida académica y de servicio a la sociedad.

La universidad cuenta con una población estudiantil cerca de los 31 mil alumnos inscritos en los diferentes niveles educativos, distribuidos entre los 4 diferentes campus y las 11 escuelas del nivel medio superior. En los últimos 100 años la Universidad se ha encontrado en un profundo proceso de modernización y expansión que en conjunto con la transformación de su estructura académico-administrativo busca renovar y mejorar la calidad en sus sistemas educativos, donde se busca promover a equidad en el acceso a la educación e incrementar la cobertura para aumentar su presencia en el estado de Guanajuato.

1.2. Distribución de campus, sedes y escuelas de nivel medio superior

Tabla 1

Distribución Campus Guanajuato

Campus Guanajuato
Edificio Central (DDPG)
Sede Noria Alta
Sede Valenciana (DCSH)
Sede Valenciana (DCNE)
División de Ciencias Sociales y Humanidades (Lenguas)
Sede San Matías (DI)
Sede Yerbabuena (DE)
Sede los Santos (DAAD)
Sede Belén
Sede Marfil (DCEA)
Sede Pueblito de Rocha

Fuente: Elaboración propia.

Tabla 1.2
Distribución Campus León

Campus León
Campus León (San Carlos)
División de Ciencias Sociales y Humanidades
División de Ciencias de la Salud (Medicina)
División de Ciencias e Ingenierías

Fuente: Elaboración propia.

Tabla 1.3
Campus Irapuato - Salamanca

Campus Irapuato-Salamanca
Sede Deportiva Norte (Enfermería)
División Ciencias e Ingenierías
División de Ciencias de la Vida
Sede Yuriria
Centro Interdisciplinario del Noreste

Fuente: Elaboración propia.

Tabla 1.4

Campus Celaya - Salvatierra

Campus Celaya-Salvatierra
Sede Juan Pablo II
Mutualismo
Sede Salvatierra
Sede el Sauz

Fuente: Elaboración propia.

Tabla 1.5
Distribución ENMS

Nivel Medio Superior
Dirección de Nivel Medio Superior
Escuela del Nivel Medio Superior de Celaya
Escuela del Nivel Medio Superior de Guanajuato
Escuela del Nivel Medio Superior de Irapuato
Escuela del Nivel Medio Superior de León
Escuela del Nivel Medio Superior de Centro Histórico León
Escuela del Nivel Medio Superior de Pénjamo
Escuela del Nivel Medio Superior de Salamanca
Escuela del Nivel Medio Superior de Salvatierra
Escuela del Nivel Medio Superior de San Luis de La Paz
Escuela del Nivel Medio Superior de Silao
Escuela del Nivel Medio Superior de Moroleón

Fuente: Elaboración propia.

1.3. Dirección de Servicios y Tecnologías de la Información

La DSTI surgió en el marco de la nueva estructura académico–administrativa de la Universidad de Guanajuato en el mes de octubre de 2011, con el objetivo de construir vías de comunicación entre la comunidad universitaria y con la sociedad en su conjunto.

La Dirección de Servicios y Tecnologías de la Información fue instituida para operar y mantener el funcionamiento de la infraestructura de tecnologías de la información, así como el Sistema Bibliotecario de la Universidad.

1.4. Antecedentes históricos

Es importante mencionar que la dirección de servicios y Tecnologías de la Información se integró básicamente por dos áreas de las cuales se mencionan sus antecedentes.

En 1991 surge la "Red Universitaria de Teleinformática y Comunicaciones (RUTyC)" como un proyecto innovador en la institución, cuando inicia este proyecto, la Universidad de Guanajuato era la quinta universidad en registrar su dominio ***ugto.mx*** ante el NIC.

En 1995, desaparece el proyecto RUTyC, dando paso al Departamento de Telecomunicaciones y Cómputo como una estructura formal dentro de la Institución. Las funciones de este nuevo departamento eran desplegar la conectividad en todas las dependencias administrativas y académicas de la Universidad de Guanajuato, además de proveer de servicios de red como; el correo electrónico, el acceso a la www y el soporte técnico.

En 1994 se incorpora el Departamento de Telefonía al Departamento de Telecomunicaciones y Cómputo siendo su función dar servicios de voz que satisficieran las necesidades de la Institución.

En enero de 2004 fue creada la Coordinación General de Sistemas y Telecomunicaciones, dependiente de la Secretaría Administrativa quedando integrados los departamentos de Telecomunicaciones, Telefonía e Informática.

En enero de 2009 se cambió la estructura orgánica en la Universidad de Guanajuato a un modelo por Campus y un Colegio de Nivel Medio Superior con una Rectoría General, impactando a la estructura de la Coordinación General de Sistemas y Telecomunicaciones la cual se desintegra, quedando en diferentes Secretarías; como Coordinación de Telefonía, Departamento de Telecomunicaciones y Departamento de Sistemas de Información.

En diciembre de mismo año, se crea la Dirección de Tecnologías de la Información la cual se compone por el Departamento de Telecomunicaciones y la Coordinación de Telefonía, su visión

se plasma sobre el despliegue de las Tecnologías de la Información y Comunicación a toda la comunidad Universitaria.

Por otro lado, en 1995, se creó la Dirección General de Apoyo Académico, esta Dirección tomó en sus manos los servicios bibliotecarios y de telecomunicaciones.

En 1999, se unió a dicha dependencia administrativa la recién creada Dirección de Archivos y Fondos Históricos.

Entre 2004-2005 durante el periodo del Rector Arturo Lara López, desapareció la Dirección General de Apoyo Académico.

En 2009 la Dirección de Apoyo Académico, se conforma por los departamentos de Sistema Bibliotecario y Fondos Históricos y Biblioteca Armando Olivares Carrillo, además de apoyar de manera conjunta las acciones de la Coordinación del Archivo General.

En octubre de 2011, se crea la Dirección de Servicios y Tecnologías de la Información, cuando debido a cambios en la estructura administrativa y en base a las crecientes necesidades de la comunidad universitaria, se decide fusionar la Dirección de Tecnologías de la Información con la Dirección de Apoyo Académico.

1.5. Funciones

- Operar, mantener y proyectar los servicios bibliotecarios y de telecomunicaciones de la Universidad de Guanajuato con la máxima disponibilidad y eficiencia;
- Administrar la Biblioteca Central para emitir lineamiento de operación que se reflejen en el óptimo funcionamiento de las Bibliotecas que conforman el Sistema Bibliotecario de la Universidad de Guanajuato;
- Proyectar, gestionar y mantener el acervo bibliográfico de la Universidad;
- Facilitar y asegurar el acceso al acervo bibliográfico requerido por profesores y estudiantes en el desempeño de sus actividades académicas;
- Proyectar y garantizar la disponibilidad de los servicios de telecomunicaciones a la comunidad universitaria;
- Mantener el buen funcionamiento de los equipos alternos de energía y los enlaces de banda ancha de la red de telecomunicaciones de la Universidad;
- Difundir y atender los servicios que ofrece la Dirección para optimizar el uso adecuado de los recursos, así como atender los requerimientos de la Secretaría de Gestión y Desarrollo.

1.6. Misión

La Dirección de Servicios y Tecnologías de la Información es la encargada de operar, mantener y proyectar los servicios relativos a la infraestructura de telecomunicaciones, así como a la infraestructura del acervo bibliográfico en colaboración con las instancias universitarias en apoyo a las funciones sustantivas de la Universidad de Guanajuato.

1.7. Visión

Constituir un eje dinamizador en recursos tecnológicos y servicios de la información académica de vanguardia bajo un esquema de innovación continua. Dotar a la Universidad de Guanajuato con una infraestructura tecnológica de punta y dinámica, que satisfaga la creciente demanda de servicios de tecnologías de la información cubriendo las expectativas de la comunidad universitaria, así como tender al liderazgo entre las instituciones de educación superior a nivel nacional en los rubros de Tecnologías de la Información.

1.8. Valores

- La verdad
- La libertad
- El respeto
- La responsabilidad
- La justicia

1.9. Organigrama

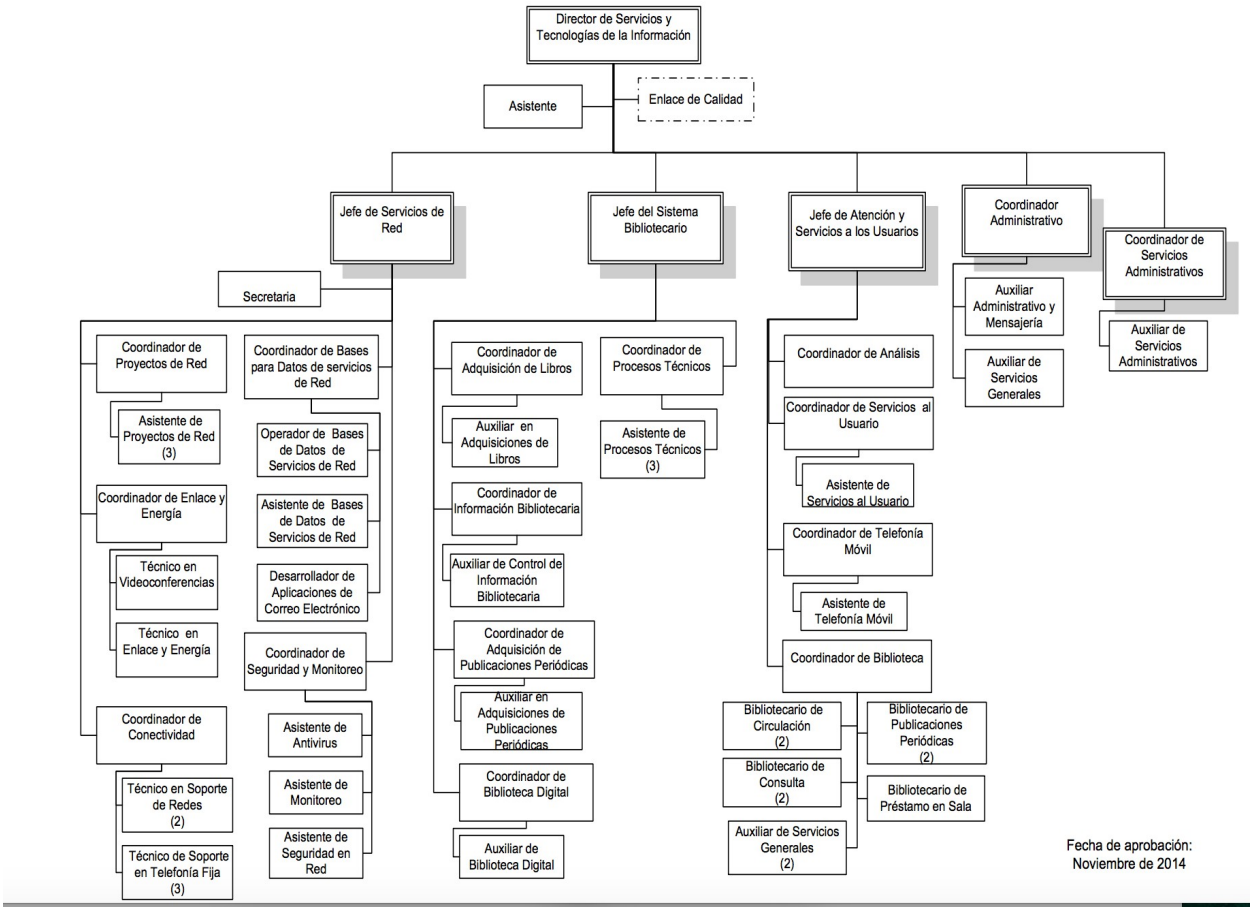

Figura 1. Organigrama de la DSTI. Fuente MO-DTI -01 (Rev.02-2014, p. 11).

1.10. Coordinación de Seguridad y Monitoreo

La Coordinación de Seguridad y Monitoreo dirige sus acciones, esfuerzos en proteger y monitorear la infraestructura de red de los Campus y Sedes de la Universidad de Guanajuato del mal uso, actos malintencionados e incidentes relacionados con la seguridad de la red para mantener y asegurar la disponibilidad del servicio de internet e intranet a los usuarios aplicando metodologías, uso de herramientas y estándares internacionales que nos ayuden a asegurar la confidencialidad , integridad y disponibilidad de los servicios de red.

1.11. Funciones

- Promover y proponer la incorporación de medidas tecnológicas y metodologías que contribuyan a mejorar la calidad de los servicios educativos dentro de la Institución.
- Formular y presentar las propuestas de normas, políticas y proyectos para mejorar, optimizar los servicios de red y proporcionar un ambiente seguro que provea la integridad de la información que transmite por la red.
- Administrar y supervisar el tráfico que transita por la red Institucional para proporcionar la seguridad requerida en las unidades y dependencias de la Universidad.
- Realizar estudios de viabilidad, compatibilidad y rentabilidad para apoyar la toma de decisiones en la propuesta de adquisición de software y hardware que fortalezca los esquemas de seguridad de la red institucional.
- Realizar un monitoreo permanente con el apoyo de herramientas tecnológicas de seguridad y monitoreo, para garantizar un servicio seguro y óptimo de red e internet.
- Proporcionar soporte técnico en la instalación, configuración, administración y utilización del antivirus institucional.
- Definir, evaluar y proponer la implantación de mecanismos de protección y seguridad de la infraestructura institucional, en coordinación con los demás departamentos de la DSTI
- Apoyar en el crecimiento de infraestructura para las redes locales, metropolitana y de área amplia en conjunto con las coordinaciones correspondientes para asegurar que la infraestructura este a la vanguardia de las nuevas tecnologías cubriendo las necesidades actuales y futuras de los clientes.
- Identificar y aplicar acciones de mejora continua en el área para mantener altos estándares de calidad en los servicios que se ofrecemos.
- Definir, evaluar y proponer metodologías para los procesos de diagnóstico de vulnerabilidades en los sistemas.
- Mantener estrecha comunicación con instituciones externas para promover acciones de colaboración de beneficio mutuo.

1.12. Organigrama

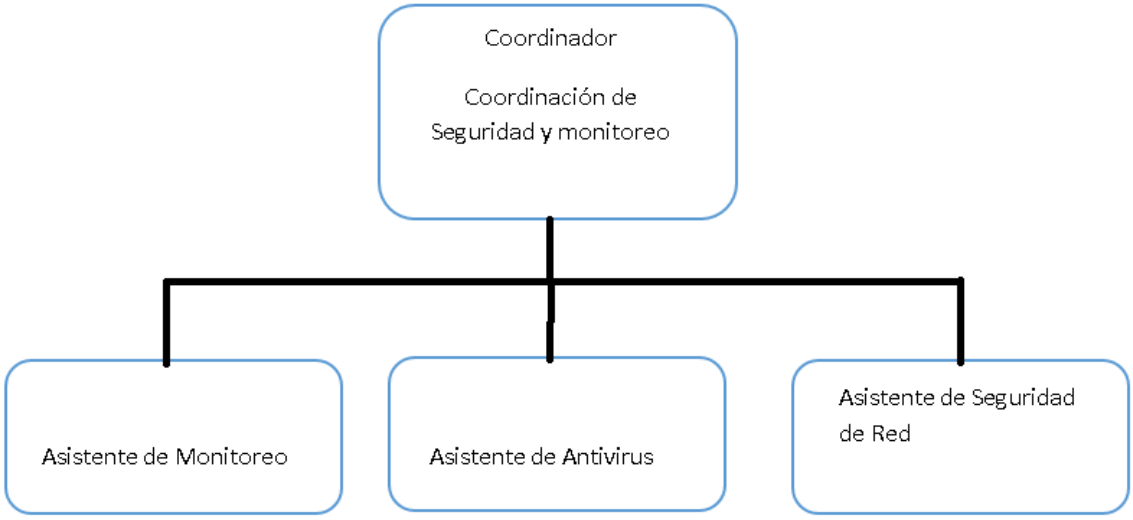

Figura 1.2. Organigrama de la Coordinación de Seguridad y Monitoreo. Fuente MO-DTI -01 (Rev.02-2014, p. 11).

1.13. Actividades de asistente de antivirus.

- Realizar la revisión, mantenimiento y administración de los servidores que alojan las consolas de antivirus para mantener un servicio óptimo.
- Realizar la revisión, mantenimiento y administración de las consolas de antivirus para facilitar la administración de los segmentos de red a los administradores o responsables de las áreas de informática de cada Campus o Sede de la UG.
- Realizar una adecuada administración de la consola del Control Manager, que es la solución que nos sirve para administrar las consolas de Antivirus.
- Apoyar con el análisis remoto, físico de equipos y servidores infectados con algún tipo de malware como parte de las estrategias en las que se trabaja con los administradores de los diferentes Campus y Sedes de la UG.
- Realizar el análisis de comportamiento de las muestras malware en forma estática y dinámica que la solución de Office Scan de Trend Micro no detecta, para poder identificar el comportamiento del malware reciente, y así poder crear una estrategia para contener una infección masiva.
- Apoyar en el monitoreo de equipos que cuentan con el cliente de antivirus de OfficeScan, usando el firewall y revisando los logs de las alertas.

- Analizar los casos de Phishing para crear estrategias de contención de manera inmediata para su correcta contención.
- Generar de reportes detallados para los administradores sobre equipos con alguna posible infección de malware para que puedan identificarlos para aislarlo de la red y revisarlos minuciosamente.
- Informar por medio de boletines de seguridad sobre las vulnerabilidades recientes de Microsoft, Adobe, Apple, Joomla, Apache, IIS, etc.
- Realizar un análisis de los equipos y servidores que solicitan algún puerto hacia internet para poder determinar el nivel de riesgo e informarlo al responsable en caso de que se encuentre alguna vulnerabilidad critica
- Atención a incidentes relacionados con la seguridad informática (SPAM, malware, DDOS, Botnets, Url's Maliciosas, ataques externos y servidores comprometidos.)
- Realizar campañas de capacitaciones presenciales o virtuales para que el personal se encuentre capacitado para enfrentar incidentes de seguridad cuando se requiera.

2. SEGURIDAD INFORMATICA

2.1. Seguridad

El termino seguridad proviene del latín *securitas* que significa cualidad de seguro, pero en un término más amplio se refiere a un ambiente estable donde se presume la inexistencia de peligros, temores y daños hacia las personas y a sus pertenencias, dando así un sentido de tranquilidad y confianza.

La seguridad es el segundo eslabón en la pirámide de jerarquías de necesidades de Abraham Maslow; en si la seguridad es algo abstracto es una sensación que tanto los seres humanos como los animales perciben, que se obtiene tras haber realizado o haber tomado ciertas medidas que nos alejan del peligro y eliminan de cierta medida la sensación de miedo, dependiendo del entorno donde se presente esta situación y se puede percibir de manera individual o grupal.
En la actualidad la seguridad tiene varias especialidades y está orientada a diferentes áreas como por ejemplo la seguridad industrial, la seguridad social, la seguridad pública y muchas más ramas, pero en nuestro caso nos enfocaremos en la seguridad informática.

2.2. Seguridad informática

La seguridad informática podría definirse como el conjunto de métodos y normas que son destinados a la protección de la información, sistemas informáticos e infraestructura de comunicaciones resguardando su disponibilidad, integridad y confidencialidad.

2.3. Objetivo

Es mantener la integridad, disponibilidad, privacidad, control de acceso de la información y de la infraestructura física y lógica. Todo esto se implementa con la ayuda de normas, metodologías, protocolos, herramientas, etc.
Los estándares apoyan en la gestión de la seguridad en ambientes complejos donde requiere que se administren las tecnologías de manera integral.

2.4. Incidentes frecuentes de seguridad informática en la UG

SPAM: Se le suele conocer como correo basura o correo no deseado, y algunas veces hacen referencia a direcciones de correo desconocidas o falsas. Y se le usa básicamente para en el envío de correo electrónico masivo con fines comerciales o de publicidad, aunque últimamente se usa para realizar estafas o cibercrimenes.

-----Original Message-----
From: Webmail Help Desk [mailto:[redacted]michoacan@inah.gob.mx]
To: undisclosed-recipients:
Subject: Última Advertencia: Estimado Webmail Usuario

Última Advertencia: Estimado Webmail Usuario,

Esto es para informarle que su cuenta de correo electrónico ha excedido su límite de almacenamiento. Usted no será capaz de enviar y recibir correos electrónicos, su cuenta de correo electrónico se eliminará de nuestro servidor. Para evitar este problema, te recomendamos que actualices tu buzón de más espacio.

Para la actualización, haga clic en el enlace de abajo y llene la completa para actualizar su buzón de correo

==========> http://tinyurl.com/[redacted]

Después de 24 horas sin recibir ninguna respuesta de usted Vamos a desactivar su buzón.

Gracias por usar Webmail
Copyright © 2014 Webmail Help Desk
Webmail Center Actualización Técnica.

Figura 2.1. Correo de SPAM. Fuente Correo de SPAM recibido.

Phishing: Es un tipo de ataque se basa en la ingeniería social, engañando a las personas haciéndolas creer que están ingresando a una página legitima pero que en realidad es una página idéntica a la original, pero con la diferencia que esta es usada para robar datos, desde la cuenta de acceso a redes sociales, datos personales y hasta datos bancarios. Generalmente los usuarios nunca o muy rara vez toman en consideración revisar la dirección de la página, se dejan llevar por la apariencia, por ejemplo y si la página parecer tener todas sus imágenes o logos en su lugar como los recordamos

en la última visita, pues damos por hecho que es la página original y que segura. Por ejemplo, la dirección de la página real www.facebook.com y una página falsa seria www.wfacebook.com, que tiene una "w" es una página diferente ya que se encuentra con otro dominio, pero tienen exactamente el mismo contenido que hace que pase desapercibida para los ojos inexpertos del usuario común y provoca que el usuario caiga en la trampa, este ataque también es usado para generar correos aparentemente provenientes de direcciones legitimas que tienen objetivos malintencionados.

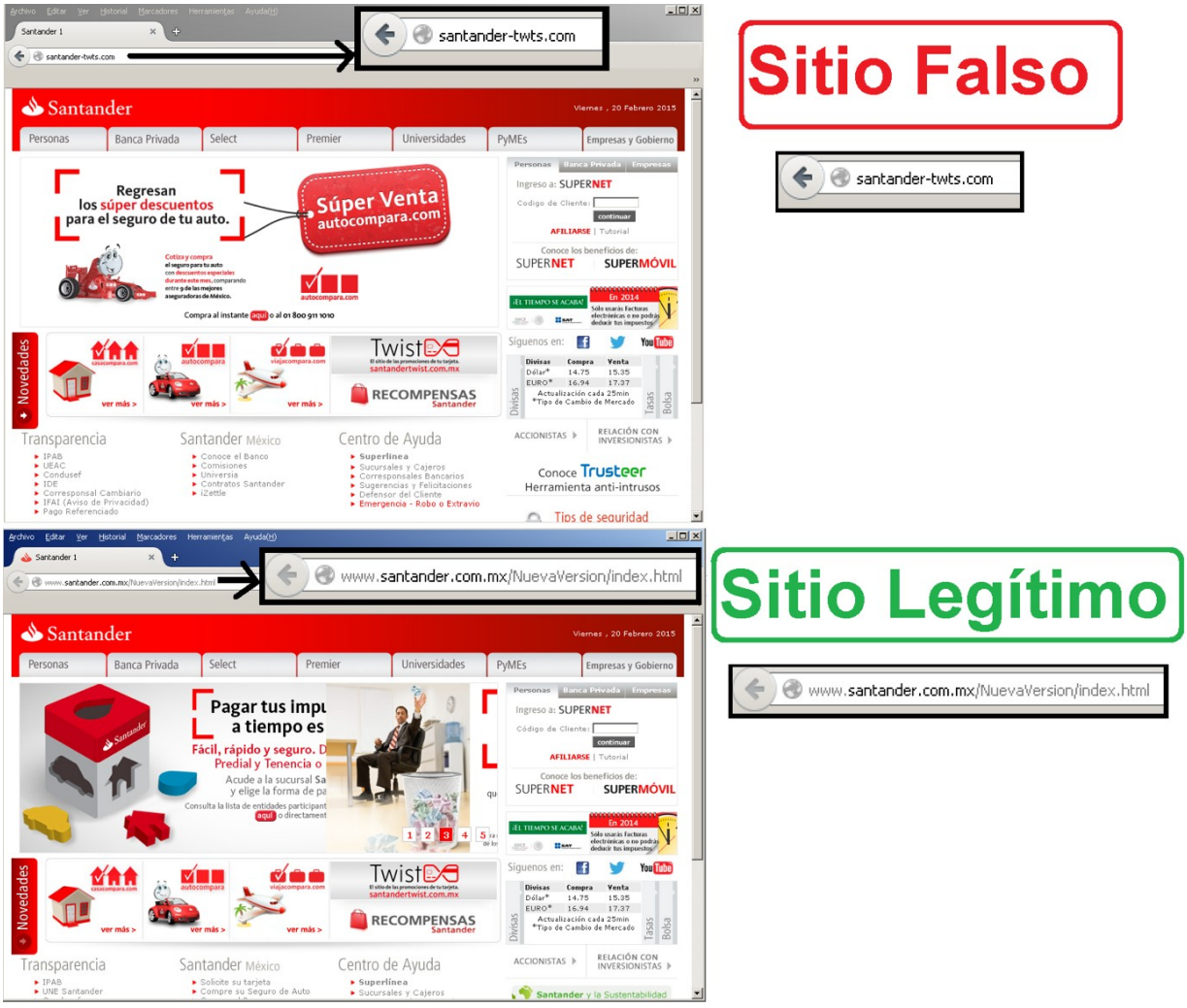

Figura 2.2. Sitio Falso de Phishing. Fuente elaboración propia.

Equipo con la seguridad comprometida (Equipo hackeado): En algunas ocasiones los cibercriminales después de lograr vulnerar un equipo o algún servidor que no contaba con las medidas de seguridad suficientes o las actualizaciones más recientes, pueden ser accedidos remotamente realizar alguna actividad ilegal o malintencionada, que van desde el envío de SPAM, distribución de malware, ataques de DOS, ataques de fuerza bruta o para montar sitios web falsos en algún subdirectorio con el objetivo de robar información o para distribuir pornografía; cualquier tipo de actividad es considerada ilegal ya que se realiza sin el consentimiento del administrador. Aunque esto se realiza sin el conocimiento del administrador, él y la empresa son los responsables de todos los daños que esto llegue a provocar, por este motivo los cibercriminales realizan estas actividades de otros equipos de manera anónima ocultando su identidad y controlando el equipo a través de conexiones remotas ocultas con diferentes técnicas de anonimato para dificultar su rastreabilidad.

Int. Entrada	Origen	Común	Destino	Int. Salida	Paquetes	Percent	% Utilizado
16	148.214.[illegible].30	http (80 TCP)	213.199.179.156	13	12.00 p	0.23%	0.0000%
16	148.214.[illegible].30	http (80 TCP)	static-148-244-43-141.alestra.net	13	6.00 p	0.21%	0.0000%
16	148.214.[illegible].30	https (443 TCP)	111.221.74.27	13	7.00 p	0.21%	0.0000%
16	148.214.[illegible].30	https (443 TCP)	157.55.130.150	13	7.00 p	0.20%	0.0000%
16	148.214.[illegible].30	https (443 TCP)	111.221.74.18	13	6.00 p	0.18%	0.0000%
16	148.214.[illegible].30	https (443 TCP)	157.55.235.158	13	7.00 p	0.18%	0.0000%
16	148.214.[illegible].30	https (443 TCP)	64.4.23.156	13	7.00 p	0.18%	0.0000%
16	148.214.[illegible].30	https (443 TCP)	65.55.223.15	13	7.00 p	0.18%	0.0000%
16	148.214.[illegible].30	http (80 TCP)	64.4.23.147	13	9.00 p	0.17%	0.0000%
16	148.214.[illegible].30	https (443 TCP)	64.4.23.147	13	9.00 p	0.17%	0.0000%
16	148.214.[illegible].30	https (443 TCP)	213.199.179.154	13	7.00 p	0.17%	0.0000%
16	148.214.[illegible].30	https (443 TCP)	157.55.235.140	13	4.00 p	0.14%	0.0000%
16	148.214.[illegible].30	https (443 TCP)	111.221.77.153	13	4.00 p	0.14%	0.0000%
16	148.214.[illegible].30	https (443 TCP)	157.55.235.147	13	4.00 p	0.14%	0.0000%
16	148.214.[illegible].30	http (80 TCP)	111.221.74.27	13	6.00 p	0.14%	0.0000%
16	148.214.[illegible].30	http (80 TCP)	157.55.235.158	13	6.00 p	0.13%	0.0000%
16	148.214.[illegible].30	http (80 TCP)	157.55.130.145	13	6.00 p	0.12%	0.0000%
16	148.214.[illegible].30	http (80 TCP)	213.199.179.154	13	6.00 p	0.12%	0.0000%
16	148.214.[illegible].30	https (443 TCP)	111.221.77.143	13	4.00 p	0.12%	0.0000%
16	148.214.[illegible].30	https (443 TCP)	157.55.235.161	13	4.00 p	0.12%	0.0000%
16	148.214.[illegible].30	https (443 TCP)	157.55.130.158	13	4.00 p	0.12%	0.0000%
16	148.214.[illegible].30	http (80 TCP)	64.4.23.156	13	6.00 p	0.12%	0.0000%
16	148.214.[illegible].30	http (80 TCP)	65.55.223.15	13	6.00 p	0.12%	0.0000%
16	148.214.[illegible].30	http (80 TCP)	111.221.77.142	13	6.00 p	0.12%	0.0000%
16	148.214.[illegible].30	http (80 TCP)	157.55.130.150	13	6.00 p	0.12%	0.0000%
(What is this?)					1.95 Kp	96.15 %	0.0008%
(from conv tables)					2.11 Kp	100 %	0.0009%

Figura 2.3. Equipo comprometido. Fuente log de herramienta de monitoreo.

Infecciones de malware: Dentro la UG las infecciones por malware más comunes a las que nos enfrentamos son realizadas por medio de los dispositivos extraíbles (USB), pero también se han presentado infecciones por correo SPAM y en ocasiones por realizar instalaciones de software pirata ya que en su mayoría contienen "Cracks o activadores" que generalmente se encuentra infectados por algún tipo de malware, que por eso no es de extrañarse que en la mayoría de los casos soliciten deshabilitar el antivirus para poder ejecutarlo de manera adecuada.

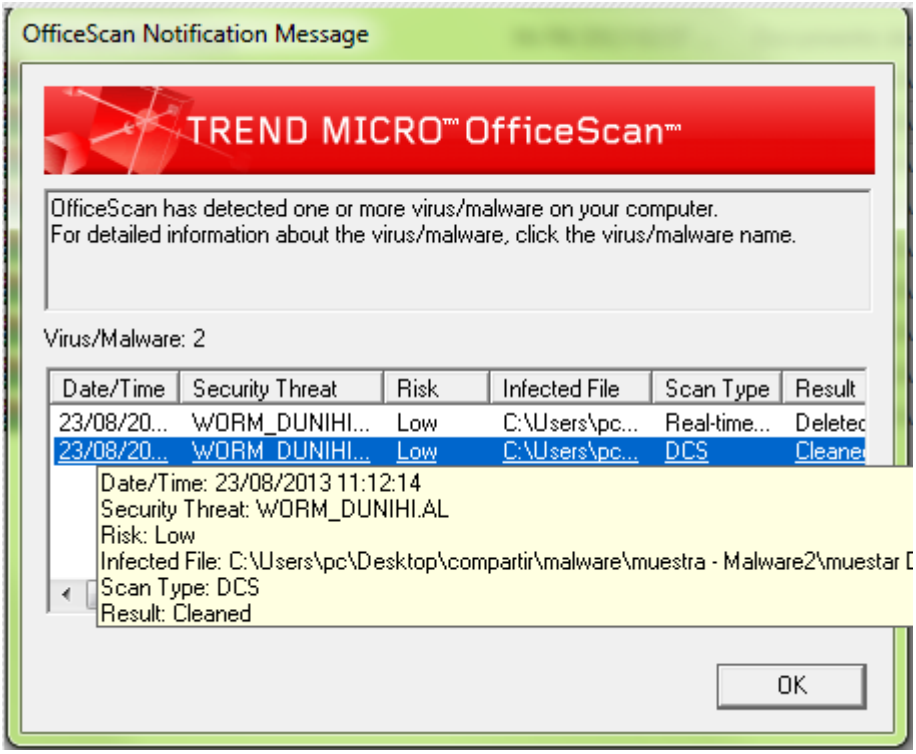

Figura 2.4. Alerta de infección por malware. Fuente ventana de alerta de antivirus.

Botnets: Son redes formadas por bots o equipos zombis, que son alimentadas por equipos infectados por malware, y son controlados de manera remota para realizar ciertas actividades ilegales. En ocasiones el mismo bot puede realizar tareas de espionaje en el equipo del usuario e incluso pueden recibir instrucciones para realizar ataques masivos como DDOS de forma simultanea contra algún sitio web.

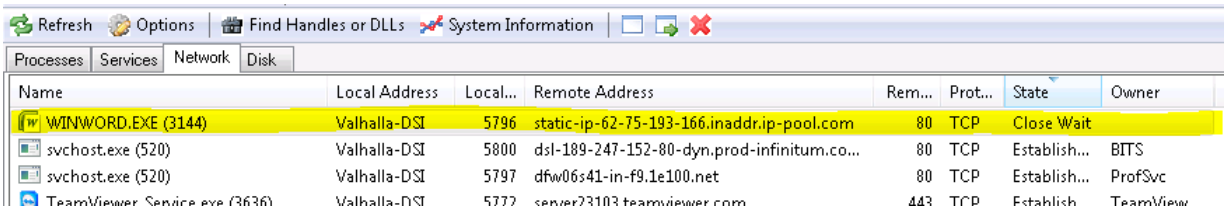

Figura 2.5. Equipo que forma parte de una Botnet. Fuente impresión de pantalla de un análisis de malware.

Defacements: Es una palabra inglesa que significa desfiguración y se usa para catalogar a los servidores web comprometidos, a los que se les realizaron cambios no autorizados en el archivo index que muestran alguna leyenda o firma de algún hacker que pudo ingresar al sitio a causa de una vulnerabilidad en el código o en los servicios. Usualmente se usar para realizar algún tipo de protesta o actividades de hacktivismo.

Figura 2.6. Mirror de un Defacement de una página web. Fuente mirror del sitio www.zone-h.org.

3. MALWARE

3.1. Malware

Es un término genérico para referirse al software malicioso o dañino que lleva a cabo actividades no deseadas y sin el consentimiento del usuario. El primer tipo de malware que se creo fue llamado virus de ahí el nacimiento del "antivirus" el software que nos ayuda a protegernos contra las infecciones u ataques de los diferentes tipos de malware, aunque contar con alguno no es garantía de protección, se recomienda tener alguno instalado con licencia vigente y que además se encuentre actualizado para reducir el riesgo de alguna infección.

El malware cada vez es más sofisticado y además es multiplataforma, a esto me refiero que ninguna plataforma puede escapar del software malicioso, anteriormente era encontrado solo en Windows, pero ahora se puede encontrar en plataformas como Linux, Solaris e incluso Mac OSX sin dejar atrás los sistemas móviles como Android y IOS.

3.2. Clasificación de malware

El malware como todas las cosas se encuentra catalogado para poder diferenciarlos dependiendo las actividades que realizan.

Adware: Son programas que no está catalogados como maliciosos pero se encuentran dentro de la categoría de software no deseado, ya que generalmente se instala sin permisos del usuario al instalar algún otro programa de algún sitio web de descargas gratis, y su función principal es mostrarnos publicidad, este tipo de software puede bajar e instalar más adwares, y generar ventanas emergentes mientras navegamos por internet donde se nos muestra mucha publicidad entorpeciendo nuestra experiencia de navegación y provocando que el equipo se vuelva lento.

Spyware: La función de los spyware es recolectar información del equipo infectado, ya sea archivos de algún tipo de formato o incluso puede estar a la espera de cierta información para enviarla a atacante o ciberdelincuente.

Troyanos: Se les nombra de esta manera al tipo de malware que va oculto dentro de programas que asemejan ser legítimos y se valen de técnicas de engaño para que puedan ser ejecutado con permisos de administrador.

En la actualidad este tipo de malware es el más usado y al que recurren más los ciberdelincuentes a la hora de infectar equipos. Ya que este tipo de malware cuenta varias funcionalidades, ya sea que sean utilizados para robar datos bancarios, información personal o que sirva de una puerta trasera para poder acceder al equipo o sistema cuando se desee.

Gusanos: Se caracterizan por replicarse a sí mismos, anteriormente su funcionalidad principal era saturar al equipo y afectar su rendimiento, ahora han evolucionado y pueden propagarse e infectar el mayor número de equipos para realizar acciones malintencionadas, actualmente los encontramos comúnmente en los dispositivos USB ya que es un medio muy efectivo para poder realizar una infección masiva.

Rootkit: El rootkit es un tipo de malware que su funcionalidad principal es generar persistencia en el sistema y tiene como objetivo obtener los máximos permisos de ejecución para poder adherirse a algún archivo fundamental del propio sistema, esto le permite permanecer oculto ante las soluciones de antivirus y realizar tareas como por ejemplo servir de puerta trasera o para alguna actividad malintencionada. Este es uno de los tipos de malware más difícil que erradicar y algunas veces es necesario reinstalar el sistema nuevamente.

Backdoors: También llamados puertas traseras y su función principal es la de mantener un acceso permanente para acceder al sistema cuando se requiera, para poder instalarse en los equipos suelen usar a los troyanos para aumentar sus posibilidades de éxito.

Rasomware: Este tipo de malware es unos de los más críticos desde mi punto de vista, ya que al infectar el equipo inmediatamente lo secuestran tomando el control, para posteriormente mostrar una leyenda en la pantalla que algunas veces dice que el equipo fue bloqueado por entidades como la policía federal en el caso de México, la interpol o alguna otra autoridad por supuestamente violar alguna leyes sobre pornografía y que para poder hacer uso del equipo nuevamente se requiere pagar "una multa" con alguna cantidad de dinero, en algunos casos me toco verificar algunos de estos equipo donde solicitaban un deposito en el OXXO de 800 pesos, pero eso no es todo nos llegamos a encontrar con otra variante más critica que actualmente se encuentra en auge y que cifra completamente los archivos de todo el sistema con protocolos de cifrado muy fuertes que hacen

casi imposible la recuperación de la información y posteriormente solicitan un pago en bitcoins para poder acceder a los archivos nuevamente, realizar el pago no asegura la recuperación de la información, en este es caso es imposible poder rescatar los datos, por lo que se recomienda tener un respaldo de los archivos en una unidad externa al equipo.

Rogueware: Generalmente suele presentarse en forma de antivirus o algún software de reparación de errores del sistema pero en realidad no lo es, y suele usar técnicas de ingeniería social para convencer al usuario de que el equipo se encuentra infectado o en el caso de los programas de reparación de errores muestra problemas críticos en el sistema; y para poder raparlos requieren que el usuario pague por el licenciamiento del software que generalmente lo muestran muy barato para alentar el usuario a comprarlo y supuestamente poder reparar el equipo, pero muchas veces se usan para robar datos de tarjetas de crédito para fines maliciosos.

Keylogger: También se le conoce como capturador de pulsaciones, y es un software que tiene la función de almacenar y enviar todas las pulsaciones que se realizan en el teclado del equipo, como por ejemplo todas las contraseñas de acceso, historiales de chat y cualquier cosa que se escriba en el teclado. También nos podemos llegar a enfrentar a keyloggers físicos que son dispositivos parecidos a una memoria USB que es indetectable para cualquier sistema o antivirus existente, se conecta entre el teclado y el equipo; esto requiere acceso físico al equipo para conectarlo y extraerlo.

3.3. Infecciones frecuentes de malware en la UG

Los principales métodos o canales de infección del malware a los que nos enfrentamos en la UG son por medio dispositivos extraíbles y por datos adjuntos en el correo electrónico que aparentan ser archivos legítimos, algún documento en formato de Word o pdf que al utilizar la ingeniería social se aprovechan de la confianza del usuario y le hacen creer que es un archivo común y corriente para que no levante sospecha, pero al abrirlo resulta ser dañino ya que contienen un código malicioso escondido en su interior que infecta el equipo o descarga algún otro tipo de malware.
También enfrentamos infecciones provocadas por realizar instalaciones de programas que son descargados de sitios donde ofrecen programas de paga de manera gratuita o por descargar canciones que miden 10 kb de redes P2P e incluso por medio de las redes sociales con los famosos

links con noticias controversiales de algún tópico actual por ejemplo, una publicación de la muerte de algún artista famoso, donde te solicitan descargar algún tipo de plugin o complemento de video que es supuestamente obligatorio para reproducir el video pero en realidad es un tipo de malware disfrazado.

3.4. Tipos de análisis de malware

Cuando encontramos algún tipo de malware que no es reconocido o detectado por la solución del antivirus institucional, se procede a realizar un análisis del mismo para poder determinar su funcionamiento y conocer su comportamiento para crear alguna estrategia de contención y detener la infección de la mejor manera posible; paralelamente o casi de inmediato se empaqueta la muestra y es enviada a los laboratorios de análisis de malware de las solución de antivirus para puedan realizar su análisis correspondiente y con ello publicar la firma de detección o el patrón de comportamiento para que el antivirus pueda detectarlo y eliminarlo. Usamos dos tipos de análisis para las muestras de malware dentro de la UG, que en un momento describiré.

3.5. Análisis estático

El análisis estático se encarga de analizar la muestra sin que el archivo sea ejecutado, para poder realizar este procedimiento se recomienda tener un equipo que se encuentre desconectado de la red o crear un laboratorio en algún ambiente virtual.

Como parte del proceso se extraen datos del ejecutable como por ejemplo su fecha de creación, la firma del software, el hash u md5 para poder corroborarlo con la plataforma de www.virustotal.com que nos ayuda a corroborar la información con las firmas de malware de aproximadamente 56 motores de antivirus.

También se le realiza un análisis de ingeniería inversa con el apoyo de un debugger para extraer el nombre de las funciones y así tener una idea de qué tipo de actividades realizaba como por ejemplo verificar si tenía alguna función de realizar impresiones de pantalla o poder capturar las pulsaciones del teclado.

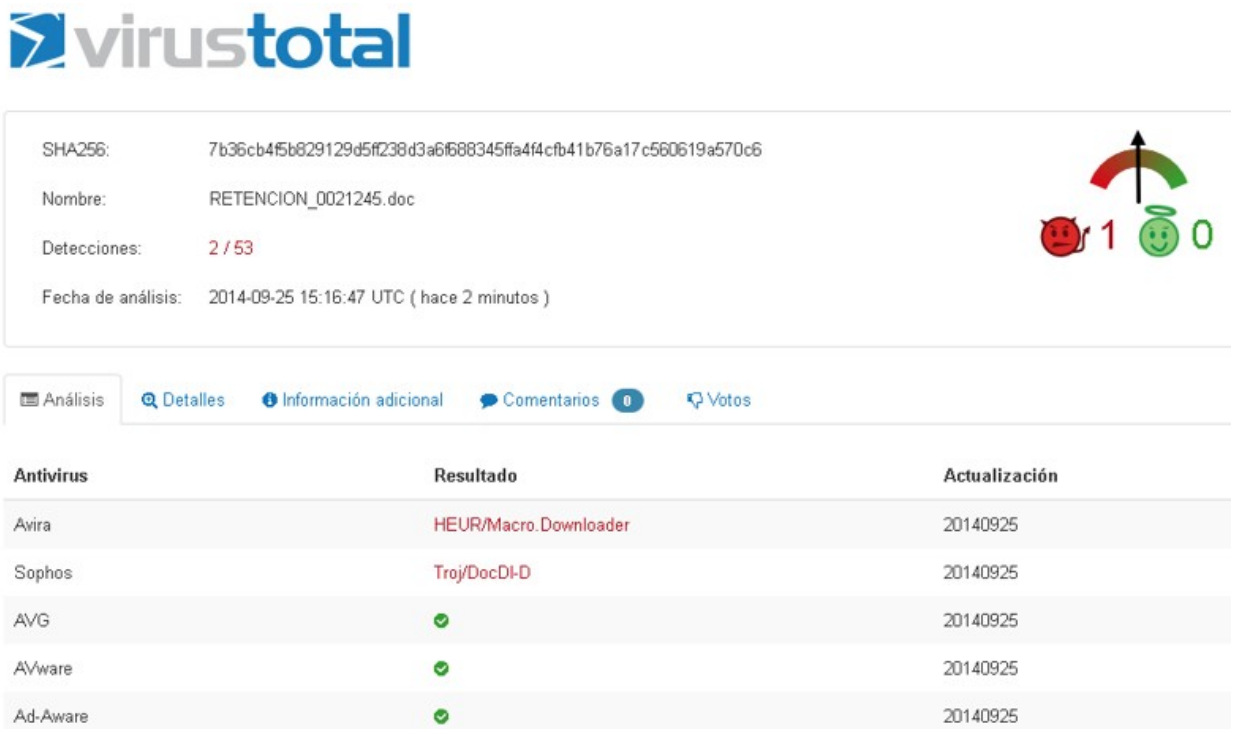

Figura 3.1. Análisis estático en el servicio de virustotal. Fuente impresión de pantalla del sitio www.virustotal.com.

3.6. Análisis dinámico

Este tipo de análisis realiza lo contrario a lo que hace el análisis estático, ya que en este procedimiento si se ejecuta el malware, ósea nos referimos a infectar un equipo para poder realizar el análisis de su comportamiento en tiempo real.

En este análisis se verifica si al ejecutarse el archivo sospechoso descarga algún otro complemento del malware, se revisan tipos de archivos y llaves en el registro que se crean en el equipo, también verificamos los puertos de comunicación y protocolos que utiliza para poder comunicarse con el servidor de comando y control en el caso que se tratara de un malware con la función de Bot.

Como en el análisis estático aquí también se recomienda realizar este análisis en un equipo que no tenga información que podamos poner en riesgo y que no esté conectado a internet o que se encuentre en una red aislada.

Anteriormente este procedimiento se realizaba en máquinas virtuales por la facilidad de crearlas muy rápidamente, eran fácil y practico disponer de una máquina virtual que contar con un equipo físico a disposición para realizar una infección, conforme realizábamos los análisis comenzamos a notar que algunos tipos de malware tienen la función de poder determinar si se encuentran en un

ambiente virtual, si lograban detectar que encontraban en una máquina virtual no se ejecutaban de manera completa, esto lo realizaban como medidas de protección anti análisis.

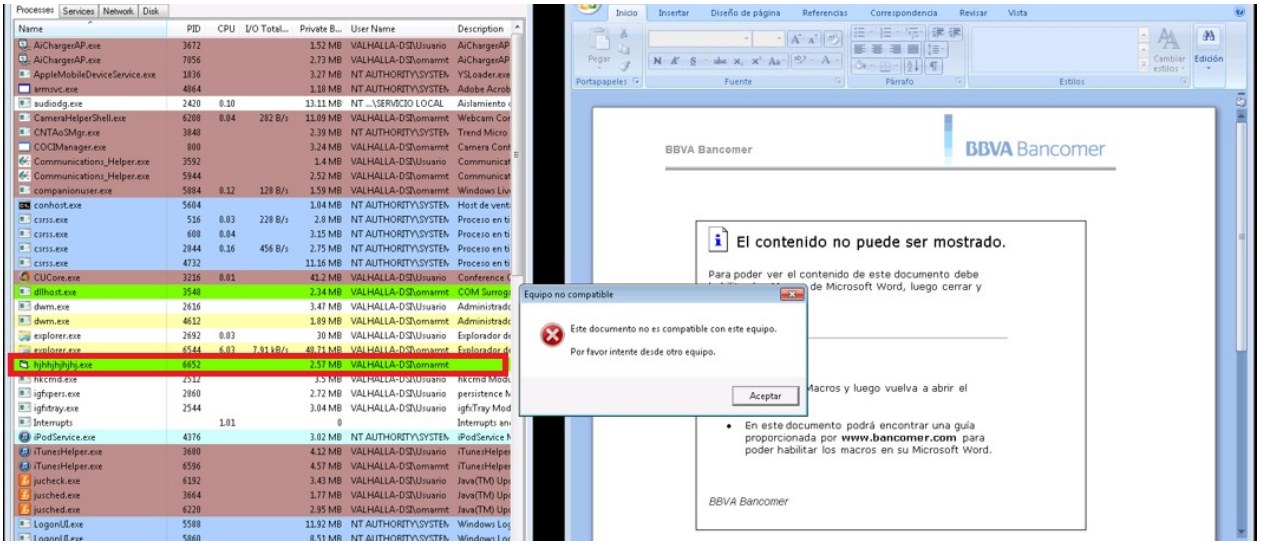

Figura 3.2. Análisis dinámico de un archivo infectado. Fuente impresión de pantalla de un análisis de malware.

4. ANTIVIRUS

4.1. ¿Qué es un antivirus?

La solución de antivirus nació en los 80's y se creó como la primera línea de defensa contra los virus. Se instalaba en el equipo para poder protegerlo y desinfectarlo en dado caso que tuviese algún tipo de malware.

Las funciones principales de este software son detectar, contener y eliminar o poner en cuarentena algún archivo o aplicación sospechosa para su respectivo análisis antes de ser utilizado. El malware ha ido evolucionando de manera vertiginosa y los antivirus tienen que estar al día con la detección, con ello han tenido que implementar más métodos de detección y desinfección contra los diferentes tipos de malware.

4.2. Funcionamiento

Su método de funcionamiento es básicamente realizar un escaneo del equipo generalmente dos o tres veces por semana dependiendo de la solución o del usuario, buscando patrones en los archivos o aplicaciones del sistema que indiquen una infección, incluso algunas veces pueden detectar un posible ataque por medio de la red o incluso detectar algún troyano escondido en algún software que parece legítimo.

Los Antivirus han desarrollado el escaneo por las hashes o firmas de los archivos, esto es para verificar si por ejemplo a algún troyano que fue catalogado como troyano.gererico.243 encontrado en el archivo de Word Tareas.doc se le cambio el nombre del archivo a proyectos.doc tiene el mismo contenido o sea el mismo hash que verifica la integridad del mismo pudiendo ahorrar tiempo en el análisis.

Otra forma de detección que se realiza es por medio del escaneo en tiempo real, este tipo de escaneo es permanente y no afecta el rendimiento del equipo, y ayuda detectando algún programa que se quiera ejecutar automáticamente o simplemente escaneando los nuevos archivos que se descargan, esto es parte de la seguridad complementaria para proteger el equipo.

El escaneo heurístico es una alternativa realmente muy efectiva, generalmente siempre tiene que salir algún tipo malware para después obtener la firma para poder detectarlo, aquí es donde entra este tipo de análisis, lo que realiza básicamente es verificar el comportamiento de los archivos y aplicaciones en tiempo real, por ejemplo un archivo de Word que al abrirlo realizar una conexión a una dirección IP de Rusia, este comportamiento no es normal así que se toman medidas de

contención a pesar de que no sea conoce nada este virus o algún procedimiento para poder eliminarlo es contenido en el momento y posiblemente enviado a sus laboratorios de análisis de malware.

También tienen la funcionalidad de protegernos cuando navegamos en internet o cuando descargamos algún tipo de software; lo que realizan es verificar cada sitio web que visitamos para verificar si no cuenta con algún reporte de distribución de malware, de envío de SPAM o algún reporte de que es una página de Phishing.

4.3. ¿Qué es un antivirus "EndPoint"?

Un antivirus Endpoint es la versión empresarial de los antivirus, se usa regularmente en las empresas que tienen una gran cantidad de equipos o en las cuales se requiere llevar un control sobre la seguridad de cada equipo de forma centralizada y detallada, como por ejemplo los bancos, escuelas u alguna empresa.

Este tipo de solución se administra desde una aplicación central, donde cada cliente de antivirus que se instaló en cada uno de los equipos, se reporta, es controlado y administrado para realizar alguna acción o simplemente mandar alertas sobre lo que ocurre en el equipo con respecto a alguna posible infección de malware.

4.4. Solución comercial Office Scan de Trend Micro

Nuestra Institución cuenta con la solución de antivirus Endpoint de la Empresa Trend Micro llamada Office Scan Endpoint Security, que nos brinda una protección integral contra cualquier ataque informático e infección de malware en los equipos y servidores.

Es compatible con las plataformas Windows, Linux y Mac; nos brinda una protección muy completa contra varios tipos de malware, además incluye Antispyware, Anti-rootkit, Firewall personal, limpieza de daños de malware a nivel de registro, integración con Active Directory, protección de medios extraíbles mediante tecnología control de dispositivos, sistema de reputación de archivos, sistemas de reputación web (WRS), bloqueo de acceso a páginas web maliciosas y de mala reputación (dentro y fuera de la red). La solución de Office Scan tiene un alcance de 2500 licencias, una licencia por equipo y contamos con una póliza de soporte por parte del Partner (Socio comercial) que es la empresa a la que se le adquirió dicha herramienta de seguridad.

4.5. Infraestructura de la solución de antivirus

La Universidad cuenta con una amplia infraestructura para realizar la administración, implementación y monitoreo de los clientes de antivirus Endpoint teniendo una gran cobertura dispersa en el estado para ofrecer una buena calidad de servicio para todos los campus, dependencias y colegios de nivel medio superior de la UG.

Se cuentan con 10 servidores DELL modelo Power Edge R510 virtualizados con la solución Esxi de VMWARE y una Workstation DELL que funge como el control manager

4.6. Cobertura de la solución por servidor y sedes

Para poder cubrir todas dependencias y Campus de la UG, se cuentan con 9 consolas de antivirus y un control manager que nos sirve para administrar las consolas de antivirus de forma centralizada. Además, contamos con un servidor llamado Smart Protection Server que es una herramienta fundamental a la hora de verificar si una url es segura o no, o nos sirve para bloquear url específicas con algún reporte de algún tipo de comportamiento malicioso.

Las consolas tienen el sobrenombre de “tepatiani” que proviene del náhuatl y significa curandero y se encuentran numeradas para identificarlas. Cada responsable de áreas de informática cuenta con acceso a una o varias consolas para poder administrar sus equipos y se puede conectar vía web con el navegador Internet Explorer.

Tabla 4.1
Cobertura del servidor tepatiani01

Cobertura Servidor Tepatiani01 148.214.8.20
Edificio de Rectoría de Campus
ENMS Celaya
División de Ciencias de la Salud e Ingenierías
División de Ciencias Sociales y Administrativas

Fuente: Elaboración propia.

Tabla 4.2
Cobertura del servidor tepatiani02

Cobertura Servidor Tepatiani02 148.214.135.5
Departamento de Ingeniería Agroindustrial (Salvatierra)
Departamento de Estudios Sociales (Salvatierra)
ENMS Salvatierra
Sede Juan Pablo (Celaya)

Fuente: Elaboración propia.

Tabla 4.3
Cobertura del servidor tepatiani03

Cobertura Servidor Tepatiani03 148.214.120.14
Departamento de Ingeniería Mecánica
Departamento de Ingeniería Eléctrica
Departamento de Ingeniería Electrónica
Departamento de Arte y Empresa
Departamento de Estudios Multidisciplinarios (Yuriria)
ENMS Salamanca

Fuente: Elaboración propia.

Tabla 4.4
Cobertura del servidor tepatiani04

Cobertura Servidor Tepatiani04 148.214.69.32
Departamento de Agronomía
Departamento de Alimentos
Departamento de Ingeniería Agrícola
Departamento de Enfermería y Obstetricia Sede Irapuato
Departamento de Ciencias Ambientales
ENMS Irapuato
ENMS Silao
ENMS Pénjamo
Centro de Vinculación con el Entorno
Imprenta

Fuente: Elaboración propia.

Tabla 4.5
Cobertura del servidor tepatiani05

Cobertura Servidor Tepatiani05 148.214.124.5
Departamento de Física
Departamento de Ingeniería Física
Departamento de Estudios Culturales
Departamento de Ciencias Aplicadas al Trabajo
Departamento de Ciencias Médicas
Departamento de Medicina y Nutrición
ENMS León Nocturna
ENMS León

Fuente: Elaboración propia.

Tabla 4.6
Cobertura del servidor tepatiani06

Cobertura Servidor Tepatiani06 148.214.16.221
Rectoría Campus León
Departamento de Psicología
Departamento de Estudios Sociales
Departamento de Gestión Pública y Desarrollo
Departamento de Enfermería y Obstetricia Sede León

Fuente: Elaboración propia.

Tabla 4.7
Cobertura del servidor tepatiani07

Cobertura Servidor Tepatiani07 148.214.3.20
Rectoría General y Edificio Central
Sede Valenciana
Sede Belén
Sede Paseo de la Presa
ENMS Guanajuato
Departamento de Lenguas
Coordinación del Archivo General

Fuente: Elaboración propia.

Tabla 4.8
Cobertura del servidor tepatiani08

Cobertura Servidor Tepatiani08 148.214.3.19
Sede Noria Alta
Departamento de Enfermería y Obstetricia Sede Guanajuato
Sede Pueblito de Rocha
Sede San Matías
Departamento de Diseño

Fuente: Elaboración propia.

Tabla 4.9
Cobertura del servidor tepatiani09

Cobertura Servidor Tepatiani09 148.214.90.5
Marfil
Departamento de educación (Yerbabuena)

Fuente: Elaboración propia.

Tabla 4.10
Cobertura del servidor Control Manager

Cobertura Servidor Control Manager 148.214.69.67
Todas las consolas de Antivirus.

Fuente: Elaboración propia.

Tabla 4.11

Cobertura del servidor Smart Protection Server

Cobertura Smart Protection Server 148.214.90.61
Todas las consolas de Antivirus.

Fuente: Elaboración propia.

4.7. Funcionamiento

Su funcionamiento está basado en la gestión, control y administración centralizada. Una vez que el cliente de antivirus correspondiente se ha instalado, automáticamente se reporta al servidor que está dentro de su cobertura donde toma la configuración y se actualiza, una vez conectado se puede revisar el estatus del equipo en el servidor y verificar si tiene alguna alerta o algún conflicto con algún tipo de software.

Cada consola tiene una cobertura específica y a cada consola le corresponde ciertos segmentos de red, esto es con la finalidad de llevar un mejor control, por ejemplo en la consola tepatiani01.ugto.mx contamos con la cobertura al segmento de red 148.214.8.0/24 , en la consola se crea un grupo donde se agrupan todos los equipos con ese segmento de red y así cada administrador o responsable del área de computo puede conectarse vía web a la consola de administración para poder revisar, monitorear o mandar alguna instrucción a los equipos dentro de los segmentos de red que están dentro de su responsabilidad.

Las consolas a su vez se conectan al servidor de Control Manager donde descargan las actualizaciones más recientes, esto es para optimizar el ancho de banda y evitar que cada consola de administración tenga que descargar las actualizaciones de manera independiente teniendo más control. Otra de las funciones primordiales y que nos sirve para la toma de decisiones son los reportes que se generan automáticamente de manera semanal donde nos avisa acerca de los equipos y redes con mayor incidencias o algún información importante que podría poner en riesgo la organización algún activo.

Además, también contamos con el servidor de Smart Protection Server que se encarga de verificar la reputación de las url's y de los archivos que manejan los usuarios.

Cada consola se encuentra conectada a este servicio adicional que nos protege bloqueando oportunamente los sitios web que cuentan con algún reporte de comportamiento malicioso, además

aquí podemos bloquear algún sitio que se considere inapropiado e incluso alguna url de Phishing que nos hayamos recibido por correo electrónico obteniendo de esta manera una capa más de seguridad

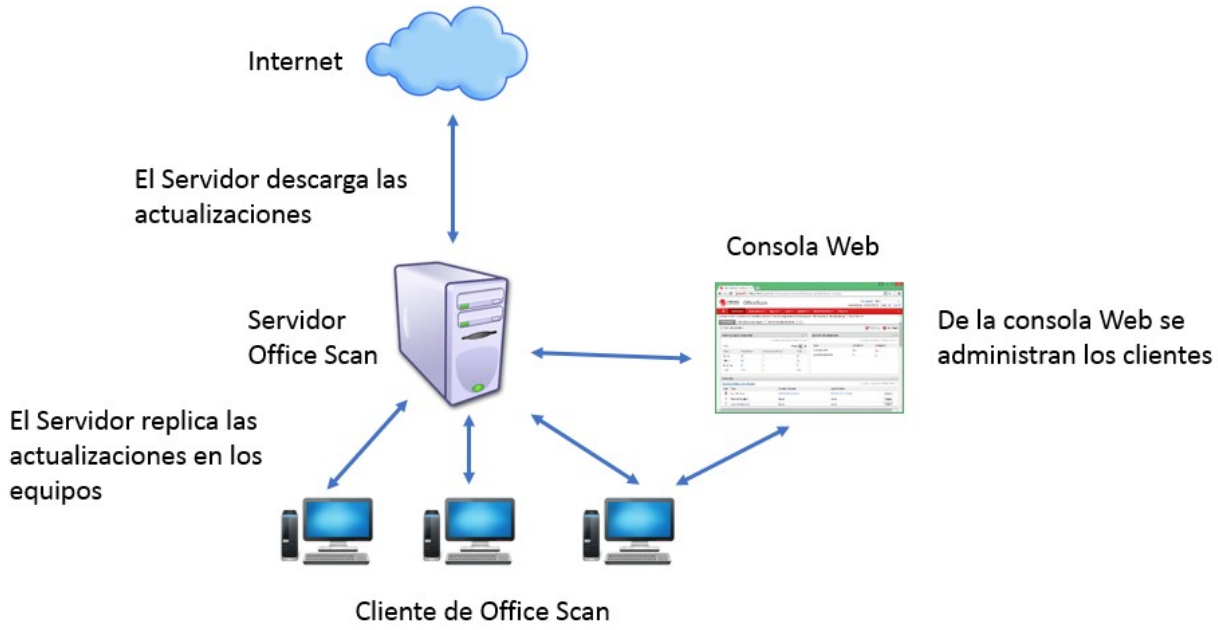

Figura 4.1 Funcionamiento de la consola de administración. Fuente elaboración propia.

4.8. Consola de administración

Cuando iniciamos sesión en la consola de administración nos aparece el "Dashboard" que es un módulo donde nos presenta un resumen del estatus de los equipos, en esta sección nos encontramos con el "Top" de los equipos con más incidencias de infección, el top de los tipos de malware más identificados, los clientes que no están conectados a la consola y muchos datos que nos dan un panorama general de la seguridad y de lo que está pasando en tiempo real que nos ayuda a poder tomar decisiones más precisas.

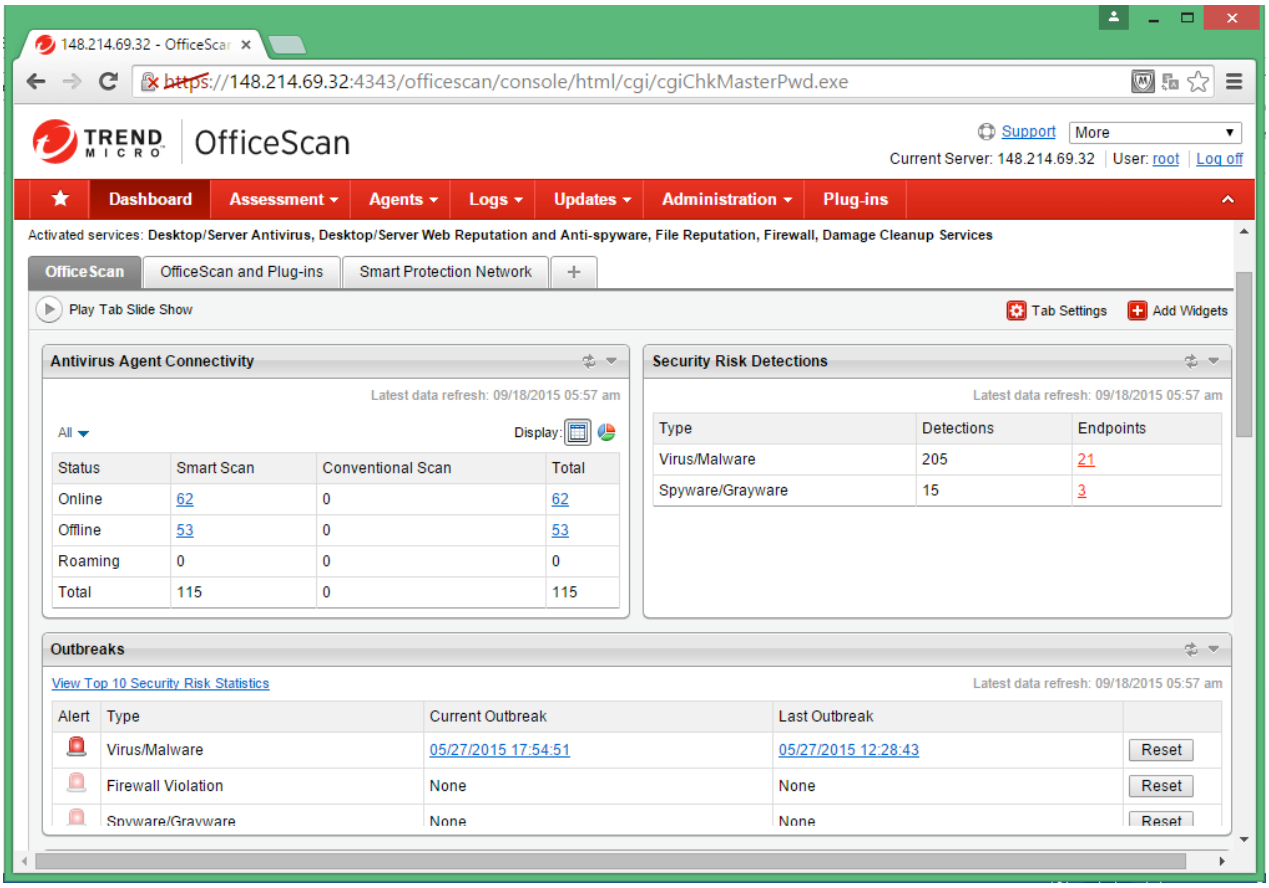

Figura 4.2. Consola web de la administración del antivirus. Fuente consola de antivirus.

4.9. Módulos de la consola de administración

La consola de administración cuenta 5 módulos principales de los cuales se despliegan varios submenús para realizar diferentes actividades.

4.10. Módulo "Assessment"

El módulo de "Assessment" se encarga de realizar un análisis de los agentes con el fin de verificar el estatus del motor de antivirus y revisar que todo se encuentra funcionando adecuadamente, además realizar un escaneo en la red y verifica cuales equipos no cuentan con el agente de antivirus instalado.

Esto nos sirve como datos estadísticos, de control y preventivo en dado caso que el agente se encuentre dañado y para la creación de estrategias más adecuadas para el despliegue de los agentes en los equipos de cómputo y servidores dentro de la red Institucional.

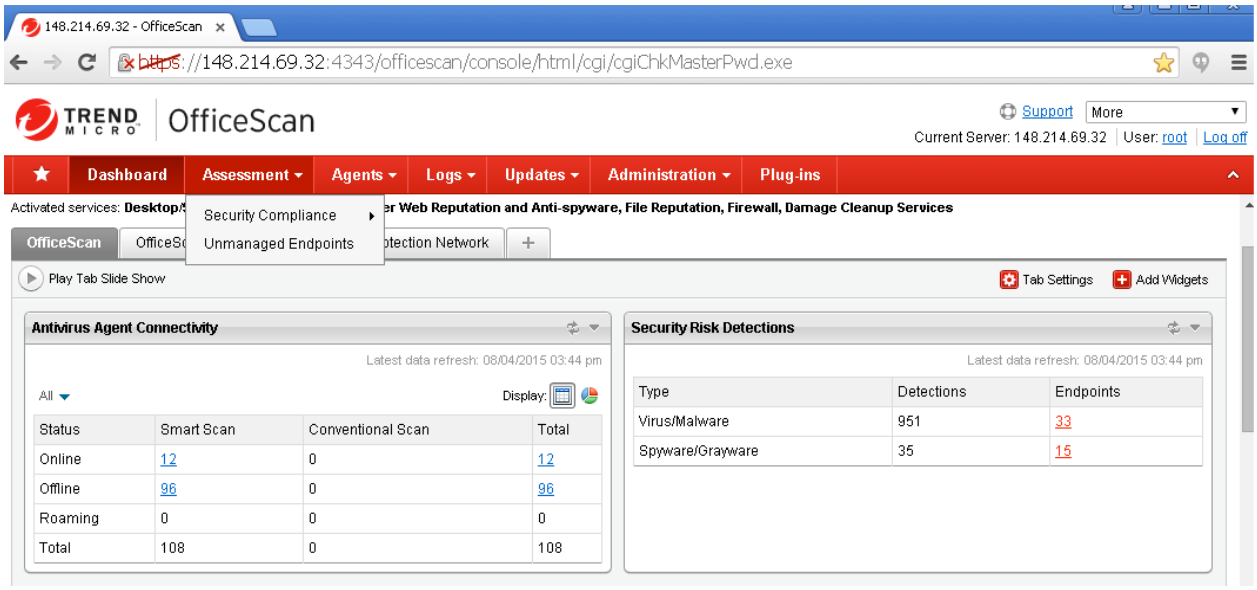

Figura 4.3. Módulo "Assessment" de la consola web de la administración del antivirus. Fuente consola de antivirus.

4.11. Módulo "Agents"

En este módulo es donde se encuentra las funciones principales de la administración, control y gestión de todos los clientes de antivirus. En esta sección se pueden realizar tareas de escaneo programado o escaneo inmediato en caso de que tengas algún reporte o alerta de comportamiento extraño, además se pueden generar políticas en el firewall para algún equipo en particular o para algún grupo.

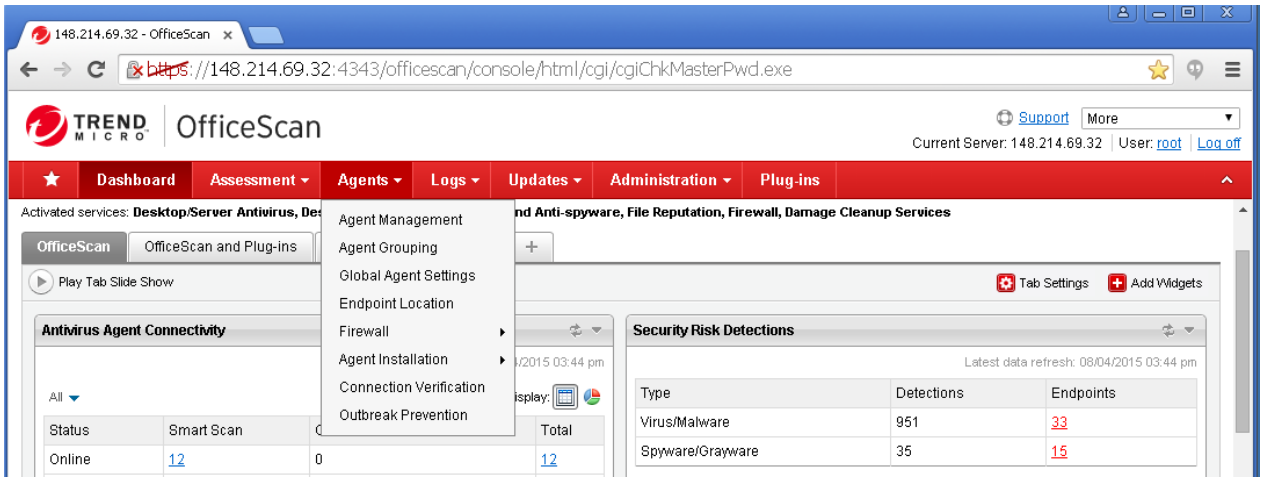

Figura 4.4. Módulo "Agents" de la consola web de la administración del antivirus. Fuente consola de antivirus.

4.12. Módulo “Logs”

En este módulo es donde se realiza la verificación de los logs de los diferentes tipos de alertas, es esta parte podemos realizar el monitoreo de los equipos en tiempo real, y están granular que lo podemos realizar para un grupo en particular, categoría de alerta en particular o de algún equipo en específico.

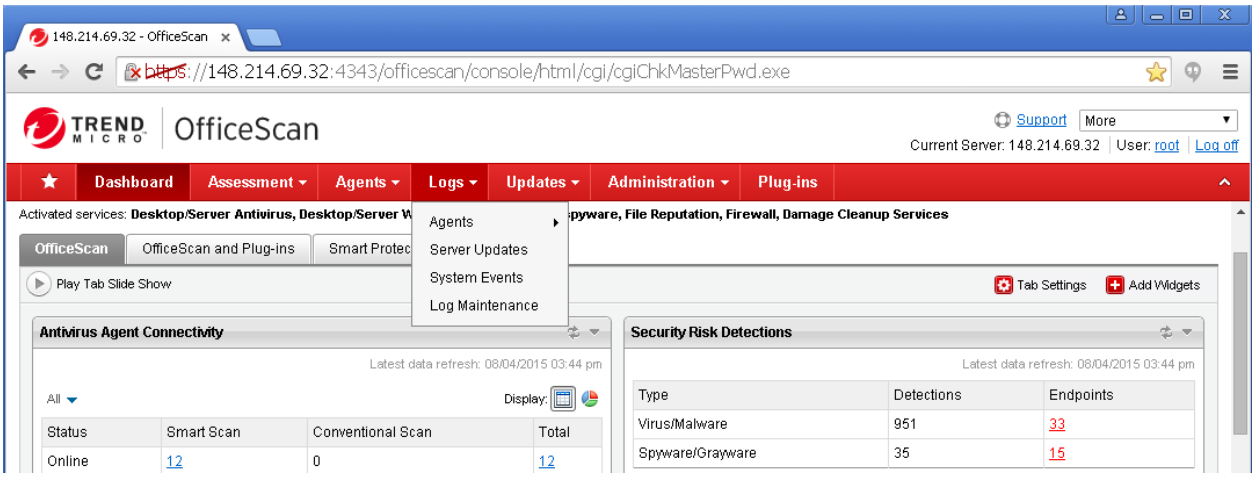

Figura 4.5. Módulo “Logs” de la consola web de la administración del antivirus. Fuente consola de antivirus.

4.15. Módulo “Updates”

En este módulo se gestionan las actualizaciones de los clientes de antivirus y de manera predeterminada se cuenta con la configuración para que los clientes se actualicen cada dos horas diariamente, además podemos identificar a los equipos que tengan algún problema con las actualizaciones para poder revisarlo más detalladamente.

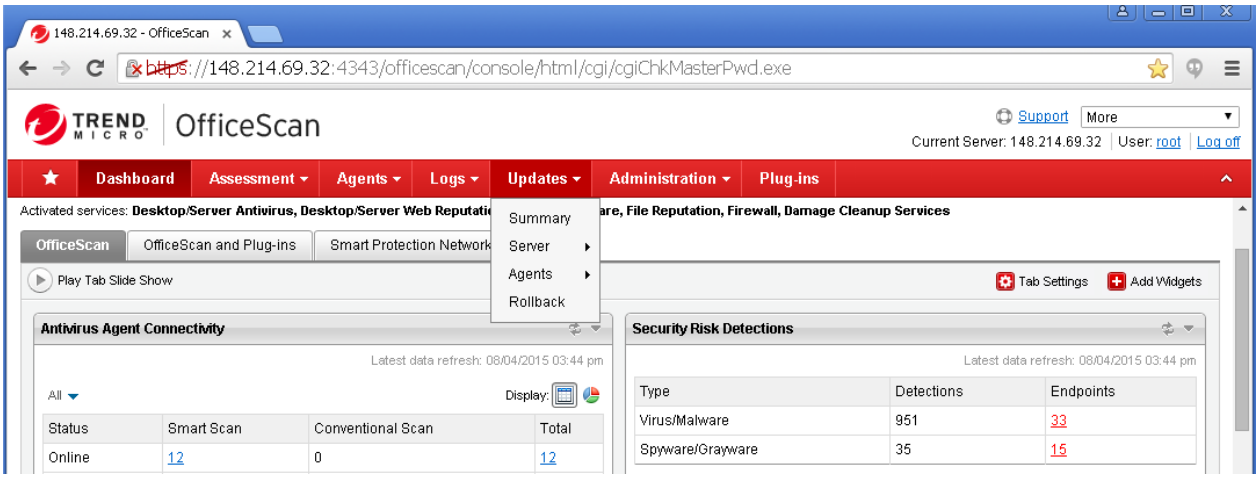

Figura 4.6. Módulo "Updates" de la consola web de la administración del antivirus. Fuente consola de antivirus.

Módulo "Administration"

En este módulo se gestiona la administración de la consola, además es donde se generan las cuentas de acceso y se asignan los permisos correspondientes para los administradores.

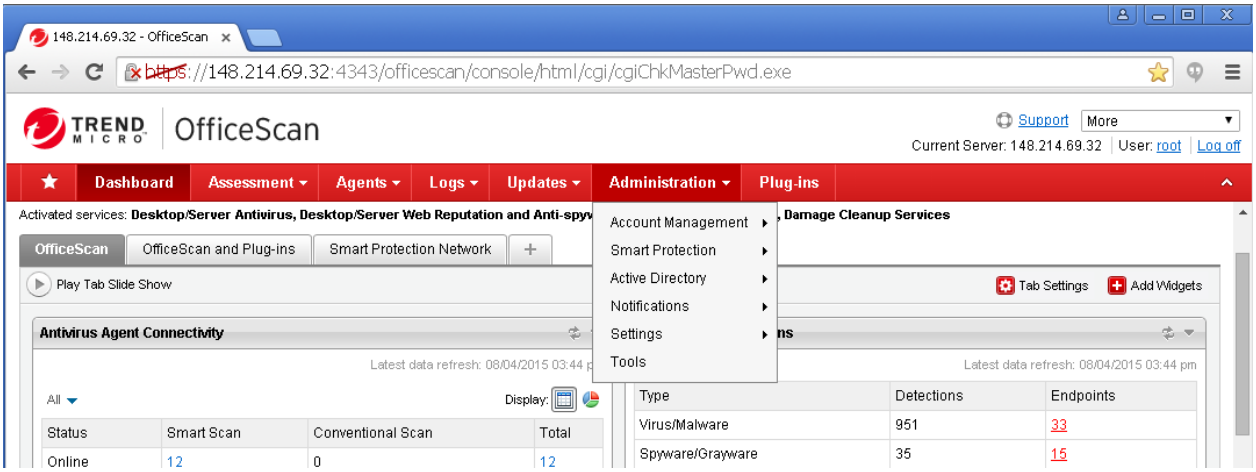

Figura 4.7. Módulo "Administration" de la consola web de la administración del antivirus. Fuente consola de antivirus.

5. ESTRATEGIAS DE SEGURIDAD EN LA UG

5.1. Estrategia de seguimiento y soporte de la consola de administración del antivirus

Para propiciar el trabajo en equipo con los diferentes responsables de las áreas de informática, se les ha proporcionado una cuenta de acceso a la consola de administración de Office Scan, para que puedan realizar las tareas de gestión y monitoreo de los equipos de los cuales son responsables u ofrecen soporte técnico.

Se les proporcionaron permisos de administración del módulo de "agents" solo a ciertos grupos que se encuentran en los segmentos de red que ellos administran, de los cuales tienen las opciones de verificar logs, realizar implementación de la configuración que ellos crean más adecuadas tomando como base una plantilla de configuración genérica, además de configurar políticas en el firewall, realizar escaneos inmediatos, así como programar un escaneo semanal entre muchas más opciones. En todo este proceso de administración los vamos asesorando paso a paso en caso de que les surgiera algún tipo de duda durante alguna implementación.

También se les ha proporcionado cursos de capacitación presenciales y remotos tanto en el manejo de la consola como en el manejo de incidentes como por ejemplo que hacer cuando tenemos un equipo infectado, qué hacer cuando nos enfrentamos a algún tipo de malware que no es detectado y se requiera realizar algún análisis más profundo, para posteriormente realizar tareas de desinfección manual con la finalidad de reducir el riesgo de que se propagué el malware y que evitar que se ponga en peligro la información del usuario.

5.2. Estrategia para contener y manejar las amenazas en la red

En la capa de red contamos con varios IDS (Intrusion Detection System) que nos ayudan a monitorear el tráfico de la red Institucional determinando si algún equipo presenta algún tipo de comportamiento anormal o malicioso, incluso si algún equipo se encuentra bajo algún tipo de ataque.

Una vez que se genera una alerta de un equipo que presente un comportamiento sospechoso se procede a realizar un reporte con el mayor número de información posible que nos pueda resultar útil para realizar las medidas correspondientes de contención. Para después compartirlo con el administrador para que estén enterados de los detalles y posteriormente nos apoyen en ubicar el equipo, proceder a realizar la revisión y desinfección correspondiente, durante este proceso se les

hace hincapié que debe de guardar una muestra del archivo del posible malware que se llegara a encontrar en el equipo para nosotros realizar un análisis más profundo si es que requiere.
Una de las medidas de contención más rápidas y efectivas es generar una política de bloqueo en el firewall local del antivirus del equipo, esta medida se realiza para evitar que se propague por la red y evitar que se genere trafico anómalo que afecte el rendimiento de la red o del servicio de internet.

5.3. Estrategia para contener y manejar las amenazas en servidores

Los incidentes con servidores son generalmente provocados por que los sistemas operativos, las aplicaciones o servicios no se encuentran actualizados o no se realizaron las configuraciones necesarias en base a las buenas prácticas para reforzar la seguridad.
Entre los ataques más comunes a los que nos enfrentamos son los "Defacements" que son las desfiguraciones de las paginas principales o index de los sitios, y que son usados generalmente por activistas para dejar un mensaje de protesta o por un hacker maligno para dejar un mensaje al administrador del sitio burlándose de la seguridad del mismo, en algunas ocasiones lo realizan con la finalidad de generar reputación en el bajo mundo del internet.
En algunas ocasiones hemos recibidos reportes de entidades bancarias como lo es el Bank Of Amerika, CERT de la UNAM y del CERT de la Policía Federal que han recibido o detectado ataques de algún equipo infectado dentro de la red institucional.
Otro de los usos que los cibercriminales les dan a los servidores después de que logran vulnerarlos, es usar poder de procesamiento que generalmente es alto para minar bitcoins o los usan en algún tipo de ataque de DOS, para distribuir malware o montar sitios falsos para realizar campañas de Phishing; ellos no se ven involucrados en este tipo de acciones ya que usan equipo de terceros.
Para realizar la contención seguimos un procedimiento similar al de los equipos que se detectan en la red interna; nos ponemos en contacto con el administrador para que revise el servidor y tome medidas de contención correspondientes e inmediatas, dependiendo del nivel de riesgo se toma de decisión de bloquear el servidor o no, ya que este tipo de equipo por su naturaleza y el tipo de servicio que pudieran ofrecer, no pueden dejar de operar ya que esto implicaría dejar a los usuarios sin algún tipo de servicio.
Una vez que se realizó la contención, el análisis y la desinfección correspondiente, nos enfocamos en realizar un análisis del servidor a nivel de puertos y servicios para identificar más posibles vulnerabilidades en los puertos abiertos y en los protocolos usados, realizando las recomendaciones

correspondientes para que puedan implementar las medidas de seguridad pertinentes o los parches en caso de que se requieran, a este proceso se le llama Hardening.
Si el servidor tiene el antivirus de Office Scan se revisan los logs y se realiza un escaneo completo para poder determinar si dejaron algún tipo de malware para complementar el Hardening

5.4. Estrategias para contener y manejar amenazas de malware en equipos de cómputo

Las infecciones de malware en los equipos de cómputo es el tipo de incidente más común al que nos enfrentamos en el día a día, y algunas veces es desencadenado por alguno de los otros incidentes o al contrario puede provocar algunos de los otros tipos de incidentes, lo que quiero decir es que están muy relacionados entre sí.
Este tipo de incidentes los recibimos por reporte de los usuarios cuando se percatan que su equipo se está comportando de una forma extraña, por alertas en los IDS, por alertas del Antivirus Institucional o por reporte de alguna organización externa.
El procedimiento a seguir cuando tenemos algún reporte de un equipo con una posible en infección, primeramente se revisan los logs en el IDS y en el antivirus para poder reunir la mayor cantidad de información posible, para conocer a que nos enfrentamos y determinar cuáles son las direcciones IPs involucradas y las urls, ya cuando se verificó este tipo de información, nos enfocamos en tratar de ubicar el equipo físicamente y contactar al administrador de esa área para darle a conocer el incidente y que nos apoye en ubicar al equipo.
Una vez que se ha localizado, procedemos a solicitar que aíslen el equipo de la red para evitar que se propagué la infección, y se le solicita al administrador o responsable de dicha área que realice una revisión exhaustiva y que nos comparta los posibles archivos sospechosos que pudieran encontrar para apoyarles en el análisis e identificar si se trata de algún tipo de malware.
Posteriormente se les pide apoyo para que realicen la desinfección del equipo y que le recomienden al usuario cambiar todas las contraseñas de las cuentas del usuario que uso en el equipo como medidas de seguridad. Para finalizar se le pide que genere un reporte detallado del incidente para poder tener conocimiento de las acciones realizadas, para en un futuro compartir esta información con algún otro administrador y tenga una referencia de cómo manejar el incidente.
Si el incidente o el reporte se considera crítico solicitamos acceso remoto o si se es necesarios nos presentamos en sitio para realizar la revisión correspondiente.

Si durante el proceso de análisis se llegara a encontrar algún tipo de malware que no es detectado por la solución de Antivirus, se extrae el archivo para analizarlo en un ambiente controlado donde realizamos un análisis estático y dinámico para identificar a qué tipo de malware nos enfrentamos, para entender su comportamiento e implementar una estrategia de contención basada en los indicadores de compromiso.

Paralelamente se envía a los laboratorios de Trend Micro en Filipinas para que sea analizado y puedan catalogarlo para liberar el patrón de detección lo más pronto posible.

5.5. Estrategia para contener y manejar Amenazas de Phishing

Cuando nos enfrentamos a incidentes de Phishing, se toman diversas medidas de contención en diferentes niveles, a nivel del equipo de usuario se le solicita que nos reenvíe el correo junto con su encabezado posteriormente se le pide que lo marque como SPAM o que lo borre.

Una vez realizado esto, al usuario afectado se le realiza una pequeña entrevista para tener más detalles, y verificar si el usuario descargo algún tipo de archivo del correo falso o si respondió el correo con algún tipo de información sensible, en dado caso que el correo tenga algún correo adjunto se le realiza el análisis correspondiente. Como medida de seguridad se le recomienda que cambien sus contraseñas de sus cuentas que usa en el equipo.

Como medida de prevención extra se realiza un escaneo remoto en el equipo del usuario con ayuda del antivirus de Office Scan por medio de la consola de administración. A nivel de red se usa el servicio de Smart Protection Server en el cual contamos con una base datos de amenazas a nivel mundial que nos ayuda en la detección y bloqueo de ulrs por medio del módulo de reputación web del antivirus, además de realizar un bloqueo a nivel de Firewall perimetral para tener una capa extra de contención.

Una vez que se implementaron las medidas de contención necesarias ahora nos enfocamos en reportar los sitios a entidades especializadas en el combate al Phishing y al fraude electrónico a nivel mundial como lo son el CERT de la UNAM, CERT de la Policía Federal, el Anti-Phishing Working Group (APWG), a google e incluso con el servicio de hosting donde se aloja el sitio; o si es el caso de algún servicio de generación de formularios gratis, ya que suelen ser usadas para este tipo de fines maliciosos.

La finalidad de este tipo de ataques es robar información personal y sensible, información bancaria y de acceso a sus cuentas de correo, para esto se valen de técnicas de ingeniería social engañando

a los usuarios con correos falsos que generalmente contiene un link de un formulario donde les piden datos personales y de acceso a sus cuentas de correo con el fin de enviar SPAM o para realizar algún tipo de fraude o ataque.

5.6. Estrategia para contener y manejar amenazas de SPAM

Algunos casos de Phishing y de malware van ligados de cierta forma con el envío de SPAM, las cuentas que son robadas por medio de Phishing o de infecciones de algún tipo de malware son usadas generalmente para enviar SPAM o distribuir correos falsos con archivos adjuntos disfrazados de facturas o algún otro tipo de engaño para sacar provecho para extraer información o comprometer la seguridad de un equipo de cómputo o móvil.

Algunos ejemplos serian el famoso correo promocionando la venta de la pastilla milagrosa viagra, algunos otros de alguna persona rica en el mundo que está a punto de morir y sin familiares que te escogió solo a ti para darte toda su fortuna, pero curiosamente necesita que le mandes algo de dinero para que pueda realizar trámites para la trasferencia del dinero a tus cuentas.

También recibimos correos que aparentemente son enviados por instituciones bancarias o alguna supuesta guía de Fedex donde te piden bajar un archivo que en realidad en un virus. El método más efectivo para el envío de SPAM es médiate el correo electrónico, aunque también podría llegar por mensajes de texto (SMS) o por medio de las redes sociales.

Cuando un equipo se encuentra infectado por algún tipo de malware, roba las credenciales de acceso a las redes sociales y cuentas de correo, esta es otra forma de acceder a cuentas existentes y legitimas para poder enviar SPAM y que puedan pasar algún filtro anti SPAM.

La forma en la que contenemos este tipo de incidentes es bloqueando todos los remitentes con reporte de envío de SPAM que se encuentran a nivel mundial en varias “Blacklist” de SPAM por medio de un servidor Anti SPAM o por algún reporte de algún usuario que nos solicita apoyo porque identifico un comportamiento extraño con su correo

Cuando nos percatamos que una cuenta de correo Institucional esta enviado SPAM inmediatamente es bloqueada y se le cambia la contraseña, después nos ponemos en contacto con el dueño de esa cuenta y se le realiza una pequeña entrevista para poder identificar si fue víctima del engaño y para identificar cual fue el correo falso y revisar quien se le envío.

Se le comentan las características de este tipo de ataque para que pueda identificar este tipo de correos fraudulentos en el futuro para que sea más consciente y pueda evitarlos.

Otro procedimiento que se realiza es verificar si sus equipos cuentan con alguna solución de antivirus y si cuenta con Office Scan creamos una política para dicho equipo en la consola de administración para monitorear el equipo y descartar que se encuentre infectado por algún tipo de malware que aún no es identificado. Si llegase a tener un virus nuevo se realiza los procedimientos de análisis, desinfección y se reporta con Trend Micro.

Una vez que revisamos todo y que el posible malware ya es detectado y contenido procedemos a habilitar la cuenta que se encontrará en monitoreo por un par de días para verificar que ya se encuentre todo funcionando adecuadamente.

5.7. Envío de boletines informativos de seguridad y de vulnerabilidades

Una estrategia de prevención que se ha implementado es el envío de boletines de seguridad vía correo electrónico donde se les informa oportunamente a cada responsable del área de computo sobre las vulnerabilidades del software más usado comúnmente dentro de la Institución.

Para que puedan estar al tanto de los nuevos riesgos y puedan tomar medidas preventivas y correctivas.

5.8. Campañas de concientización

Se han realizado campañas de concientización para la comunidad universitaria por medio de los medios informativos institucionales como lo es la revista de Gaceta universitaria, donde realizan publicaciones con un enfoque informativo para dar a conocer los ataques más frecuentes, como funcionan y como poder realizar medidas preventivas. Todos estos artículos se realizan con un lenguaje muy fácil de entender y dando a conocer que tipo de daños podemos sufrir.

CONCLUSIÓN

Después de haber colaborado 4 años en la coordinación de seguridad y monitoreo como el administrador del antivirus Institucional, me ha generado un aprendizaje enorme en el área de redes y seguridad; mi visión se ha ampliado en cuanto los riesgos a los que nos enfrentamos y con ello buscar la manera para poder combatirlos o evitarlos de la mejor manera posible. También se ha reforzado mi pasión por desarrollar actividades en el área de la seguridad informática.

Las actividades que he realizado me han dado la experiencia y los conocimientos para manejar los incidentes del día a día, así como los incidentes críticos que ponen en riesgo la infraestructura de red que puede afectar tanto la operación como la información de los usuarios, todo esto tomando como herramienta principal la solución de Antivirus.

Cabe mencionar que en esta área tan cambiante siempre es necesario capacitarse constantemente y estar al día con las noticias de los reportes de ataques que se van generando a nivel mundial, desde cómo se realizan y como se contienen para estar preparados ante cualquier eventualidad, este tipo de actividad se le denomina ciberinteligencia.

Una parte muy importante es estar al día con los reportes de nuevos fallos de los diferentes tipos de software y hardware que puede pueden afectarnos, para tener oportunidad de realizar las estrategias correspondientes de actualización o de avisar a los diferentes administradores para que tomen sus medidas preventivas.

Finalmente quisiera mencionar que contar con los últimos sistemas avanzados con respecto a la seguridad o contar con el mejor antivirus, no nos asegura que vayamos a estar protegidos en su totalidad, la mayoría de los incidentes se pueden evitar usando el sentido común. De ahí que hemos estado trabajando en realizar tareas de concientización con todos los tipos de usuarios, para prevenir cualquier incidente. Lamentablemente los mismos usuarios en algunas ocasiones no miden el riesgo y no toman consciencia hasta que les toca vivir alguna infección de malware donde algunos han perdido su información de trabajo que han estado desarrollando a lo largo del tiempo.

GLOSARIO

Ingeniería Social: Es la práctica de obtener información a través de la manipulación de las personas.

Conectividad. Capacidad de dos o más dispositivos de comunicarse entre sí.

DNS. Sistema de Nombres de Dominio.

Blacklist: Lista que se utiliza para catalogar a sitios que tengan algún comportamiento Malicioso

Hacktivismo: (un acrónimo de hacker y activismo) se entiende normalmente "la utilización no-violenta de herramientas digitales ilegales o legalmente ambiguas persiguiendo fines políticos

CERT: Proviene del inglés "Computer Emergency Response Team" es un centro de respuesta a incidentes de seguridad informática.

Hardening: Termino que se utiliza para para el proceso de seguridad un sistema, para reducir vulnerabilidades o debilidades.

Análisis Forense: Es el proceso donde se aplican técnicas científicas, analíticas y especializadas para realizar la examinación digital de evidencia de algún caso de un proceso legal o para ayudar a determinar o detectar pistas de un ataque informático

Networking. Proceso mediante el cual se conectan los dispositivos para comunicarse en red.

Seguridad informática. Área de la informática que se enfoca en la protección de la seguridad de la información y los sistemas computacionales.

Sistemas de información. Conjunto de elementos que procesan, almacenan y gestionan la información para una mejor visualización y ayuda en la toma de decisiones.

Sistema de Nombres de Dominio (DNS). Sistema que mapea las direcciones de Internet con los dominios asignados.

Tecnologías de la Información (TI). Lo relacionado con el tratamiento, almacenamiento, procesamiento, comunicación y visualización de información relacionadas con aplicaciones de hardware y software.

Ataque: Un ataque es un evento exitoso o no, que atenta sobre el buen funcionamiento del sistema.

Vulnerabilidad: Hace referencia a un fallo o debilidad de algún sistema que puede permitir ser explotada por algún atacante para causar algún tipo de daño.

Ataque DOS: Es un tipo de ataque que se enfoca en denegar el servicio, realizando más peticiones de las que se puede manejar.

IP: Significa "Internet Protocol" y en un número que identifica un equipo en una red.

Exploit: Fragmento de código que explota una vulnerabilidad.

Firewall: Es un sistema de defensa que bloquea el acceso no autorizado y al mismo tiempo controla los accesos autorizados

Debugger: Programa usado para depurar y reparar errores.

Hash: Firma de integridad de un archivo

Amenaza: Se representa a través de una persona, una circunstancia o evento, un fenómeno o una idea maliciosa, las cuales pueden provocar daño en los sistemas de información, produciendo pérdidas materiales, financieras o de otro tipo.

Bitcoin: es una moneda electrónica descentralizada.

Servidor comando y control: consiste en servidores que son usados para controlar malware.

NIC: (Network Information Center) es el encargado del registro, mantenimiento, asignación y control de los nombres de dominio.

Ciberinteligencia: Se refiere a las actividades de inteligencia en los procesos de la Ciberseguridad que se ocupan de analizar (Intenciones-oportunidades de los ciberactores) y prevenir, identificar, localizar y atribuir ataques o amenazas a través del ciberespacio.

Deepweb: Se conoce como internet profunda, al contenido de internet que no es indexado por los motores de búsqueda convencionales, debido a diversos factores.

BILBIOGRAFIAS

What is a Botnet? (s.f). Septiembre 20, 2016, de Microsoft Sitio web: https://www.microsoft.com/security/sir/story/default.aspx#!botnetsection

Botnet (s.f). Diciembre 10, 2016, de Wikipedia Sitio web: https://es.wikipedia.org/wiki/Botnet

Defacement (s.f). Noviembre 10, 2016, de Wikipedia Sitio web: https://es.wikipedia.org/wiki/Defacement

Antivirus (s.f). Noviembre 10, 2016, de Wikipedia Sitio web: https://es.wikipedia.org/wiki/Antivirus

Antivirus (s.f). Septiembre 20, 2016, de Microsoft Sitio web: https://www.microsoft.com/es-xl/security/resources/antivirus-whatis.aspx

Jesús Ramón Jiménez Rojas, Rocío del Pilar Soto Astorga. (2009). Software antivirus. Diciembre 10, 2016, de UNAM Sitio web: http://www.seguridad.unam.mx/usuario-casero/eduteca/main.dsc?id=116

Heurística en antivirus. Diciembre 10, 2016, de Wikipedia Sitio web: https://es.wikipedia.org/wiki/Heur%C3%ADstica_en_antivirus

Erika López López. (s.f.). Seguridad informática. diciembre 10, 2016, de UNAM Sitio web: http://redyseguridad.fi-p.unam.mx/proyectos/seguridad/index.php

¿Por qué estudiar en la UG? (s.f.). Noviembre 15, 2016, de Universidad de Guanajuato Sitio web: https://www.ugto.mx/campusgto/futuros-alumnos/iporque-estudiar-en-la-ug

Universidad de Guanajuato. (s.f.). Noviembre 15, 2016, de Wikipedia Sitio web: https://es.wikipedia.org/wiki/Universidad_de_Guanajuato

Tovar Baiz, Eugenia Margarita. (2014). Manual de Organización. MO-DST-01. Noviembre 10, 2016, de Universidad de Guanajuato Sitio web: ftp://148.214.34.52/formatos/Manuales/MO-2014/RG/MO-DST-01.pdf

Seguridad (s.f). Noviembre 10, 2016, de Wikipedia Sitio web: https://es.wikipedia.org/wiki/Seguridad

Marc Thouvenot. (2014). Diccionario náhuatl -español basado en los diccionarios de Alonso de Molina con el náhuatl normalizado y el español modernizado. Noviembre 28, 2016, de UNAM

Sitio web:
http://www.historicas.unam.mx/publicaciones/publicadigital/libros/diccionario/diccne_T.pdf