MONOGRAFÍA DE ESTUDIO SOBRE EL ANÁLISIS DE LA AFECTACIÓN DE LAS BOTNETS SOBRE LOS EQUIPOS DE COMPUTO PERSONALES

ANDREI LUCIANO JIMÉNEZ ARIAS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA “UNAD”

ESCUELA DE CIENCIAS BÁSICAS E INGENIERÍA

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

BOGOTA D.C

2018

MONOGRAFÍA DE ESTUDIO SOBRE EL ANÁLISIS DE LA AFECTACIÓN DE LAS BOTNETS SOBRE LOS EQUIPOS DE COMPUTO PERSONALES

ANDREI LUCIANO JIMÉNEZ ARIAS

Monografía de investigación para optar por el título de especialista en seguridad informática

Ingeniero JULIO ALBERTO VARGAS FERNÁNDEZ
Director del Proyecto

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA “UNAD”
ESCUELA DE CIENCIAS BÁSICAS E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA D.C
2018

Las ideas que se expresan en este documento

son de exclusiva responsabilidad de su autora

y no comprometen la ideología de la

Universidad Nacional Abierta y A Distancia UNAD

Nota de aceptación

_____

_____

_____

_____

_____

_____

_____

Jurado

_____

Jurado

_____

Jurado

Bogotá D.C., Octubre de 2018

DEDICATORIA

A mi familia

Especialmente a mi hijo ya que es el motor de mi vida, una razón más para seguir adelante, también a mi madre y mi padre ya que siempre han estado apoyándome y ayudándome para seguir con mis proyectos.

AGRADECIMIENTOS

Agradezco la oportunidad brindada por la UNAD para poder ampliar los conocimientos, por el apoyo de los profesores quienes a lo largo de la especialización ayudaron a la profundización de los conocimientos y sobre todo al ingeniero Julio Alberto Vargas Fernández ya que, gracias a él, a sus consejo y guías, fue posible el desarrollo de este trabajo, en el cual se puede demostrar el conocimiento adquirido.

CONTENIDO

LISTA DE TABLAS

LISTA DE ILUSTRACIONES

GLOSARIO

ADWARE: Software no deseado que tiene como finalidad el envío de contenido publicitario.

AGUJERO DE SEGURIDAD: Acceso de manera inesperada de un atacante que por lo general es utilizado para acceder a un sitio sin la autorización respectiva y en busca de realizar un acto ilícito.

AMENAZA: Evento que puede alterar el comportamiento normal de la información, causando pérdidas de información.

APLICACIONES ENGAÑOSAS: Programas que no son legítimos y que buscan vulnerar los equipos de cómputo para poder acceder a la información personal que se encuentra en los equipos de cómputo.

ATAQUE CIBERNÉTICO: Acción que busca el daño o funcionamiento no adecuado de un sistema informático con el uso de la tecnología.

BOT: Computadora individual que está infectada con malware.

BOTMASTER: Ciberdelincuente con conocimientos en seguridad informática, que tiene una botnet a su cargo para realizar actividades ilícitas.

BOTNET: Red de ordenadores que es controlada por un ciberdelincuente para realizar actividades ilícitas.

CIBERDELITO: Un delito informático es toda aquella acción, típica, anti jurídica y culpable, que se da por vías informáticas o que tiene como objetivo destruir y dañar ordenadores, medios electrónicos y redes de Internet[1].

CONFIDENCIALIDAD: Es garantizar que la información será protegida por su naturaleza, para que solo tengan acceso las personas autorizadas.

DDoS: Sigla en inglés de Distributed Denial of Service (Ataques Distribuidos de Denegación de Servicio), es el que se realiza cuando una cantidad considerable de sistemas atacan a un objetivo único, provocando la denegación de servicio de los usuarios del sistema afectado. La sobrecarga de mensajes entrantes sobre el sistema objetivo fuerza su cierre, denegando el servicio a los usuarios legítimos.

DELITO: Cualquier actividad ilegal que sea utilizada o ejecutada para acceder u obtener información sin permiso del propietario.

[1] Ciberdelitos. http://ciberdelitoss.blogspot.com/2013/06/definicion.html

DISPONIBILIDAD: Garantizar que se tiene acceso a la información de manera inmediata o en tiempos muy cortos a las personas autorizadas.

EXPLOITS O PROGRAMAS INTRUSOS: Son programas que identifican las vulnerabilidades del software para de esta manera evadir los mecanismos de seguridad que se tengan implementados para atacar un equipo.

FRAUDE: Práctica ilegal que busca utilizar la información que por lo general no es legal.

HACKER: Persona experta en el manejo de computadoras, que se ocupa de la seguridad de los sistemas y de desarrollar técnicas de mejora.

INGENIERÍA SOCIAL: práctica utilizada para engañar a los usuarios para manipularlos y hacer que den información que no debe ser divulgada para de esta manera poder acceder a los sistemas de manera “legitima”.

INSEGURIDAD: Falta de protección o de mecanismos para la protección de información y acceso a la misma.

INTEGRIDAD: Garantizar que la información es legítima y no ha sido manipulada por personal no autorizado, si se registra algún cambio debe estar documentado.

KEYSTROKE LOGGER O KEYLOGGER: Programa que tiene como finalidad la captura de actividades realizadas mediante el teclado y mouse, esto con el fin de tener los datos de cuentas como por ejemplo las cuentas bancarias o de correo.

MALWARE: Software malicioso, su objetivo es acceder o dañar el comportamiento de un computador sin el permiso del propietario.

RANSOMWARE: Software que se usa para secuestrar información.

RIESGOS: Probabilidad de que se produzca un evento y sus consecuencias negativas.

ROBO DE IDENTIDAD: Uso de datos de otra persona para cometer delitos.

ROOTKITS: Malware que es instalado con consentimiento del usuario que se le asignan privilegios de administrador, los cuales ejecutan códigos maliciosos para tener el control del equipo de cómputo, la cual abre puertas traseras para que accedan y la manipulen de manera remota.

SOFTWARE DE SEGURIDAD FRAUDULENTO O ROUGE: Aplicación que parece ser legitima que por lo general indica que limpia registros o es detector de software

malicioso, pero que en realidad da paso a aplicaciones que son basura o corrompen el sistema.

SPAM: Correo no deseado que se envía de manera masiva, más conocido como correo basura.

SPYWARE: Software que captura la información personal que se encuentra en los equipos de cómputo o las credenciales que se encuentren en las mismas.

TELNET: (Telecommunication Network). Es el protocolo de red que se utiliza para acceder a una computadora y manejarla de forma remota. El término también permite nombrar al programa informático que implementa el cliente.

VULNERABILIDAD: incapacidad de resistencia cuando se presenta un fenómeno amenazante.

RESUMEN

En el presente documento se encontrará la información relacionada con el tema de los botnets, que son, para que se usan, como pueden llegar a afectar a los equipos de cómputo, con que finalidad se utilizan, quienes las manejan y algunos tips que se deben tener en cuenta para evitar el ataque de los mismos. De la misma manera se podrán identificar los tipos de ataques que se pueden presentar por parte de los ciberdelincuentes para buscar el acceso a los equipos de cómputo para de esta manera realizar actividades ilícitas para el beneficio de los mismos.

Al conocer cómo se comportan los botnets, con que finalidad son utilizados, que consecuencia puede traer la instalación de uno de esos robots en los equipos de cómputo, se busca la concientización de los usuarios finales para que adopten buenas prácticas para la salvaguarda de la información y la protección de los equipos de cómputo y la información almacenada en los mismos.

PALABRAS CLAVE: Botnet o red de robots, ciberdelincuentes, denegación de servicios, malware, seguridad de la información, delitos informáticos.

1. TÍTULO

ANÁLISIS DE LA AFECTACIÓN DE LAS BOTNETS SOBRE LOS EQUIPOS DE COMPUTO PERSONALES

2. INTRODUCCIÓN

Teniendo en cuenta la importancia de la información que se tiene almacenada en los equipos de cómputo (pc), y que en la actualidad y por causa de la innovación y avance de la tecnología, los mismos se encuentran expuestos a constantes ataques informáticos, razón por la cual se hace necesario identificar los ataques a los que se encuentran expuestos y los controles que se pueden establecer para la protección de la información hablándolo a nivel personal o empresarial.

En la actualidad, la gestión de la información se ha optimizado de acuerdo a la automatización de procesos, esto para darle mejor usabilidad a los recursos, es por ello que se implementan en muchas ocasiones herramientas o software para la gestión de los recursos, pero en algunas ocasiones y por la misma razón, se obvian muchas situaciones o componentes dejándolos en muchas ocasiones por defecto o como es entregado por el proveedor y por esa razón no se tiene blindada toda la información. Eso conlleva a la pérdida o vulnerabilidad de los datos y de la información propia.

Otro factor que se puede presentar es que en algunas ocasiones por desconocimiento o ingenuidad de los usuarios, los equipos de cómputo pueden

quedar desprotegidos, ya que llegan a instalar aplicaciones o software que no han sido adquiridos de manera licita (pagando licencia) o descargándolos desde sitios de dudosa reputación y es en ese momento cuando pueden instalarse aplicaciones conocidas como malware que lo que buscan es acceder a los equipos para realizar actividades ilícitas como por ejemplo extraer información valiosa, o llegar a controlar el equipo para que ejecute tareas de manera automatizada por parte de un atacante.

Por lo antes expuesto, los atacantes o delincuentes buscan de todas las maneras posibles y poniendo en práctica sus conocimientos y experticia, la forma de realizar actividades que están fuera de la ley de la manera más anónima para poder obtener beneficios de manera ilícita, esto sin que las víctimas lo detecten sino hasta cuando ya sea demasiado tarde.

3. DEFINICIÓN DEL PROBLEMA

Los dispositivos electrónicos o equipos de cómputo están expuestos en todo momento a ataques que lo que buscan son las vulnerabilidades que pueda tener algún equipo para así violar la seguridad de los mismos y poder acceder a la información o a los equipos de cómputo para usarlas en tareas en beneficio del atacante.

Esto se evidencia en la mayoría de los casos porque no se tienen buenas prácticas para la gestión de la información o de la seguridad de los dispositivos, ya que se tiene la idea que a uno no lo van a atacar, porque eso solo le pasa a los demás, porque la información que tengo no es importante.

De igual manera se puede ver este tipo de vulnerabilidades cuando se instalan programas de dudosa reputación que se supone hacen una tarea pero que en realidad lo que hacen es instalar malware para que la víctima pueda ser atacada, dado que se puede modificar o denegar algún servicio de seguridad que evite este tipo de ataques.

Al ser víctima de este tipo de ataque, el botmaster o quien controla la red, puede controlar los equipos de cómputo de forma remota para usar los equipos de cómputo (pc) y de esta manera delinquir sin ser identificado.

3.1 FORMULACIÓN DEL PROBLEMA

¿El análisis de la afectación de las Botnets y su comportamiento ayudará a crear conciencia a los usuarios finales para evitar implementar medidas de seguridad y controles para que sus equipos de cómputo no se vean afectados y expuestos a delitos informáticos y a una posible pérdida de información?

4. JUSTIFICACIÓN

La tecnología es un instrumento necesario en la actualidad, ya que gracias al avance e implementación de la misma se han logrado grandes avances de la humanidad, al igual que ha sido de gran ayuda para la automatización y optimización de muchos procesos tanto a nivel empresarial como personal, pero no solo eso, sino que también ha permitido que las comunicaciones se expandan a sitios donde hace nos años no se veía posible; esto se puede evidenciar por ejemplo en el caso de los correos, que hace unas décadas solo se podía tener contacto o noticias de sitios lejanos o de difícil acceso en cuestión de días o hasta meses, pero con la implementación de las tecnologías y ajustes de medios de comunicación, ya que desde hace unos años es posible tener comunicación por medio de teléfonos fijos, con su mejora que fue el celular mediante el cual no es necesario estar pegado a un cable para la comunicación, sino que solo necesita que tenga acceso a una red y de esa manera poder comunicarse en tiempo real, otro ejemplo es el correo, que gracias al uso de las tecnologías ya se puede hacer de manera virtual o electrónica, y de esta manera las comunicaciones por ese medio se optimizaron hasta el punto de obtener información no en mese o días sino en minutos o segundos. Esto ha sido un gran avance ya que gracias a las bondades que se tienen por esto, los fabricantes presentan gran variedad de productos y de esa manera se puede acceder a equipos de cómputo para uso personal y no como hace un tiempo que solo se podía desde sitio conocidos como café internet donde se podía acceder

a los equipos solo de manera temporal ya que eran alquilados por tiempo y las personas se encontraban sujetas a disponibilidad.

Con la implementación de la tecnología, es posible estar disponible de manera virtual casi todo el tiempo, es por esta razón que en la actualidad es posible tener la mayoría de la información en servidores de correo electrónico, en la nube, o en servidores; es por esa razón que se pueden realizar transacciones bancarias en línea o trámites de la misma manera y es por ello que los ciberdelincuentes se encuentran al asecho constantemente en busca de esa información para realizar actividades ilícitas.

Es muy importante tener conocimiento en este tipo de ataques o vulnerabilidades que se pueden presentar, ya que todos están expuestos a estos ataques en todo momento y de la misma forma saber cómo se pueden evitar o corregir estas fallas que puedan tener los usuarios y así asegurar la información.

Por todo lo relacionado anteriormente, es importante que los usuarios sean conscientes en cuanto a los riesgos a los que se encuentran expuestos y de esa manera adoptar buenas prácticas para mitigar el riesgo y salvaguardar sus intereses, su información y hasta su identidad y de esta manera garantizar la integridad y disponibilidad de las mismas; de la misma manera que tener control del acceso y evitar el mismo a personal no autorizado, así evitará que ellos le den uso de manera inadecuada o a la información almacenada en los equipos de cómputo.

La ventaja de conocer los ataques es la implementación de medidas preventivas para evitarlos y crear una mejor cultura relacionada con la seguridad de la información, ya que por lo general, la única medida de seguridad que se tiene es que el computador esté en una ubicación conocida, pero no se tiene la certeza que computador puede ser atacado en cualquier momento o que puede ser ya un equipo que está siendo atacado de manera silenciosa y cuando se ha atacado, puede ser manipulado de manera remota y transparente para el dueño del mismo; al presentarse esta situación, la víctima puede estar involucrada en algún delito informático sin ser consciente de la situación.

5. OBJETIVOS

5.1 OBJETIVO GENERAL

Identificar los ataques informáticos a los que se encuentran expuestos en la actualidad los usuarios finales y el riesgo que corren al ser infectados por algún malware que los haga parte de una botnet y los tipos de delitos informáticos más comunes que se presentan y en los que se podrían ver involucrados si son parte de una Botnet.

5.2 OBJETIVOS ESPECÍFICOS

- Identificar los ataques informáticos más conocidos en la actualidad.
- Citar los tipos de malware más conocidos y utilizados por los ciberdelincuentes en la actualidad.
- Listar los delitos informáticos más relevantes de los últimos tiempos.
- Entender cómo se compromete la integridad de un equipo que se encuentre en una botnet y su comportamiento.

- Crear una guía para el usuario final donde encontrará recomendaciones para que se deben tener en cuenta con el fin de mitigar el riesgo y evitar ser parte de una Botnet o de ser parte de un delito informático.

6. MARCO REFERENCIAL

6.1 ANTECEDENTES

(ARAUZO ALMIRON, 2009) [2]En documento memoria denominado “Botnet”, trata de manera detallada toda la información básica que se debe tener en cuenta con relación a los Botnet o Red-Robot, al igual de como este tipo de red toma bastante protagonismo en el tema de la “ciberguerra” y como es el comportamiento del malware para la infección que se aplicará a la víctima.

En el trabajo de Maestría denominado “Detección y bloqueo de botnets mediante la combinación de técnicas basadas en el tráfico de red” (RIPOLL CERVERA, 2015)[3] publicado por la Universidad Nacional de Educación a Distancia, al ser un trabajo enfocado en la detección y bloqueo de ataques, se encuentra una idea más aterrizada relacionada con los ataques realizados por los botmasters y la identificación de los mismos, también se encuentran las evidencias de las pruebas

[2] Botnet. https://upcommons.upc.edu/bitstream/handle/2099.1/8692/Mem%C3%B2ria%20Arauzo%20Almiron,%20Valentin.pdf

[3] Detección y bloqueo de botnets mediante la combinación de técnicas basadas en el tráfico de red. http://www.issi.uned.es/Master_ISSI/WebMISSI/RepositorioTFM/2015/15S_MemoriaTFdM_ISW_TipoB_Juan_Enrique_Ripoll_Cervera.pdf

realizadas para detectar los ataques y como poder controlar y evitar el robo de información.

En el informe denominado “Detección de botnets basada en algoritmos genéticos” (GARCIA S. , 2011)[4], se puede evidenciar el comportamiento del tráfico de una botnet, y después de acuerdo con los datos que se tomaron se realiza un análisis del tráfico sobre otra red para identificar si se encuentra tráfico similar y se puede detectar si se encuentra algún equipo infectado como un robot. En el informe se pueden identificar los algoritmos que se utilizan para el estudio del tráfico que se encuentra dentro de la botnet.

En el artículo bimestral de la revista denominada “Punto Seguridad, seguridad en TIC” (SANCHEZ SOLEDAD & SANTILLAN ARENAS, 2010)[5], citaron temas relacionados con Botnets, donde le cita al lector los usos que les dan a las botnets, como es la comunicación entre los bots, los puertos que por lo general son usados por ese tipo de robots para que se comuniquen y un pequeño listado de botnets donde se pueden identificar la cantidad de bots que alcanzaron a tener y cuál fue el porcentaje de ataque a nivel mundial mientras estuvieron activas.

[4] Detección de botnets basada en algoritmos genéticos. https://www.researchgate.net/profile/Sebastian_Garcia6/publication/237836318_Deteccion_de_botnets_basada_en_algoritmos_geneticos/links/0c96051bc3066460e5000000/Deteccion-de-botnets-basada-en-algoritmos-geneticos.pdf

[5] Botnets. http://www.ru.tic.unam.mx:8080/tic/bitstream/handle/123456789/1726/31.pdf?sequence=1&isAllowed=y

En el proyecto denominado “Técnicas de detección y análisis de malware en entornos corporativos con sistemas Windows” (CUBIDES CORRALES, MURCIA GUZMAN, & ZAPATA PAREJA, 2015)[6], se puede ver un nivel de detalle muy dirigido a la seguridad informática, se habla de todas las vulnerabilidades a las que se encuentra expuesto el sistema en ciertos momentos, como cuando no se realiza una buena configuración o parametrización, también citan las recomendaciones que se pueden tener para la protección de los equipos de cómputo. Finalmente se ve el análisis realizado al sistema y como lo puede desestabilizar.

6.2 MARCO TEÓRICO

En la actualidad, día a día las organizaciones o cualquier persona hace uso de los equipos (personales (pc o portátiles)), los cuales se encuentran en constante riesgo por ataque de los ciberdelincuentes quienes buscan el acceso no autorizado a los equipos de cómputo para extraer información o tener control de las mismas para realizar actos ilícitos que van a beneficiarlo, es por esto que se pueden presentar fallas o vulnerabilidades en los equipos de cómputo inicialmente porque no se tiene la cultura de asegurar la información implementando mecanismos de control y seguridad; por otra parte porque no se protegen los equipos de cómputo, esto quiere

[6] Técnicas de detección y análisis de malware en entornos corporativos con sistemas operativos Windows. http://bibliotecadigital.usb.edu.co/bitstream/10819/4208/1/Tecnicas_Deteccion_Analisis_Zapata_2015.pdf

decir que se dejan de manera tal que cualquier persona pueda acceder a las mismas dado que no se tienen establecidos controles de acceso tales como usuario y contraseña y es por esta razón que se puede acceder de manera limpia a cualquiera de las mismas, también se puede ver esto cuando se instalar programas o aplicaciones sin ningún tipo de restricción o se dejan por defecto, dejando expuesto el equipo de cómputo para que pueda tener acceso o pueda ser manipulada de manera muy sencilla.

Este tipo de ataques se pueden presentar también por culpa de las personas o usuarios ya que no tienen el debido cuidado cuando están utilizando los equipos de cómputo, esto quiere decir que no tienen la cultura de escanear los dispositivos que conectan, no los vacunan o simplemente instalan aplicaciones que son gratuitas o que son descargadas de sitios no confiables, pero aun así la instalan porque les puede servir para “solucionar” algún inconveniente que tienen con los equipos de cómputo, y lo más común, es cuando se instalan aplicaciones o programas que permiten evadir o saltar la seguridad para poder hacer “legal” algún tipo de software, ya que cuando se instalan, estos inicialmente piden que se le asignen permisos de administrador y mediantes los mismos tienen acceso a registros que pueden modificar y así poder crear una puerta trasera, y es por allí donde va a realizarse el ataque.

Los ataques más conocidos en la actualidad son los realizados con software malicioso, el cual se instala cuando no se tiene cuidado con las aplicaciones que se

manejan o no se tienen establecidos controles de acceso a páginas en internet, ya que por lo general se instalan programas gratuitos que no están en un repositorio confiable, y es por este medio que los atacantes publican malware que a los ojos de los usuarios son aplicaciones normales pero que internamente al instalarse de manera silenciosa se ejecutará en segundo plano al tener permiso de administrador, puede acceder al sistema e instalarse para posteriormente iniciar el ataque, esto se puede llegar a controlar si se tiene habilitada la seguridad para la instalación de software donde tiene que darse permiso cada vez que se desee hacer esta tarea y de igual manera controlando la instalación de programas y descargándolos desde sitios seguros.

Teniendo en cuenta la importancia de la información, es necesario establecer mecanismos de seguridad que ayuden a identificar cuando el equipo de cómputo está siendo atacada y de esta manera poder salvaguardarla, es por eso muy importante tener en cuenta las buenas prácticas que se pueden establecer para la protección y disponibilidad de los activos de información en cualquier escenario, tal como puede ser en el ámbito personal que para este caso sería con los equipos que se tienen en los hogares (personales (pc o portátiles)), ya que en la gran mayoría de los casos es allí donde se tiene almacenada la información personal y familiar; también se deben establecer estas medidas de seguridad en los sitios de trabajo, esto ya que una organización tiene la información que es uno de los activos más importantes, y la misma está expuesta a ataques constantes, ya que si tienen acceso a la misma, pueden llegar a perjudicar de manera irremediable la

continuidad de la misma. Por lo anteriormente mencionado, es necesario tener conocimiento de los ataques a los que se encentra constantemente expuesta para de esta manera realizar una planeación que permita la protección y también se debe capacitar y concientizar a las personas en los hogares y a las personas de las empresas para de esta manera mantener a salvo la información y así crear una cultura que va a servirle a todos en cualquier momento.

De la misma manera es necesario realizar seguimiento a las acciones realizadas y si es necesario establecer medidas preventivas y correctivas, para esto es bueno establecer auditorias mediante las cuales se puede identificar el estado actual del manejo y tratamiento de la información, y de la misma forma se pueden implementar medidas o controles que ayuden a blindar o mitigar los riesgos que se puedan presentar.

Con la implementación de estas medidas y controles, se puede identificar de manera más sencilla los riesgos o fallas de seguridad a las que se están expuestos y de esta manera se podrá controlar el acceso a la información y se manejarán buenas prácticas para el tratamiento de la información.

Con el manejo de estos procesos, se pueden identificar dos tipos de amenazas relacionadas con este riesgo, las cuales se citan a continuación:

AMENAZA LÓGICA[7]: Aplica cuando a través de malware o virus se accede al equipo de cómputo y afecta el normal comportamiento de la misma.

AMENAZA FÍSICA[8]: Está relacionado con fallos de los dispositivos. También se relaciona con fallos físicos, los cuales pueden ser causados por el usuario como robo de información, fraude, sabotaje, o fallos como cortos circuitos, incendios, inundaciones, etc.

Para garantizar la seguridad e integridad de la información, se hace necesario conocer los ataques que se pueden presentar en la actualidad para de esta manera estar preparados para evitarlos y asegurar la misma, es por esto que se deben aplicar o establecer buenas prácticas para el tratamiento de la información; esto se aplica para todos los dispositivos que se utilizan para la comunicación (computadores, teléfonos inteligentes, tablets, etc).

De la misma manera, se debe tener en cuenta que este tipo de ataques son presentados de diferentes maneras o a través de distintos medios, mediante los cuales los delincuentes o atacantes identifican para realizar sus actos ilícitos; a continuación, se presentan los más conocidos:

[7] Tendencias 2011: las botnet y el malware dinámico. http://www.eset-la.com/pdf/prensa/informe/tendencias_2011_las_botnet_y_el_malware_dinamico.pdf

[8] Seguridad Física. https://www.segu-info.com.ar/fisica/seguridadfisica.htm

Virus: Son programas creados con la finalidad de atacar o hacer actividades que por lo general hacen que los dispositivos o los equipos de cómputo donde se instalen, se comporten de manera extraña, ya que lo que buscan es corromper los sistemas y en la mayoría de los casos atacan el sector de arranque en busca de hacer que los sistemas queden fuera de funcionamiento; de la misma forma de acuerdo con su programación, e replican en el sistema o haciendo polimorfismo para moverse entre los archivos sin ser detectado para así realizar no solo daño al sistema sino también a los archivos.

La propagación de ese tipo de archivos, mejor conocidos como malware, es en la mayoría de los casos por los medios electrónicos como por ejemplo en internet, ya que los ciberdelincuentes aprovechan este medio para manejar estos archivos en los diferentes medios como por ejemplo mediante juegos, páginas infectadas, redes sociales, etc.

Otro medio de propagación es mediante el correo electrónico, dado que es uno de los medios más utilizados en la actualidad, por su eficiencia y disponibilidad de la información. Por este medio los atacantes pueden aprovechar que las victimas en muchas ocasiones no disponen de herramientas para asegurar la información tales como antivirus, antimalware, etc., y es por esto que pueden hacer ataques de tipo phishing o con esteganografía y de esta manera pueden hacer que el malware se ejecute de manera silenciosa sin que la víctima se dé cuenta o de su autorización y así acceder a los archivos o al mismo sistema.

De la misma forma se utilizan las vulnerabilidades identificadas por los delincuentes por intermedio de la mensajería instantánea como lo fue en su momento Messenger de Microsoft, o como se puede ver en yahoo Messenger, ya que por esos medios al instalar aplicaciones con emoticones que no eran las oficiales, los usuarios estaban abriendo ventanas mediante las cuales los atacantes podían acceder a los equipos de cómputo y tener acceso a la información, en la actualidad esto se puede ver en WhatsApp, ya que al compartir archivos por este medio y no tener aplicaciones como antivirus que escaneen los mismos para validar que no sean malware, se están abriendo canales o dando aval para que ataquen y tengan control de los equipos de cómputo o dispositivos.

Por otra parte, en muchas ocasiones al instalar sistemas operativos, no se tiene la costumbre o buena práctica de personalizarlos, esto debido a que se dejan de manera genérica o como lo sugieren los sistemas y es en estos casos que los atacantes pueden tener identificados ataques zero day[9], esto quiere decir que identifican la vulnerabilidad y aprovechándola realizan ataques para acceder a los equipos de cómputo o dispositivos, estos también son conocidos como “back doors” o puertas traseras, por lo general estos ataques se realizan porque los administradores de los equipos de cómputo dejan el acceso libre por puertos como el 80 o 25 (telnet).

[9]¿Qué es un exploit de día cero? https://latam.kaspersky.com/resource-center/definitions/zero-day-exploit

Otra vulnerabilidad que se presenta es cuando se instalan RootKits[10], los cuales tienen la característica de asignar permisos de administrador mediante los cuales se puede tener acceso a toda la información y configuración y de esta manera poder manipular el equipo de cómputo a su antojo, por lo general los usuarios instalan este tipo de software para homologar algunas restricciones que deben ser validadas para su legalidad.

Finalmente el uso de las redes P2P[11] o punto a punto, ya que por intermedio de estas, los equipos de cómputo se comportan como cliente y servidor en cualquier momento, y son utilizadas para compartir información o intercambiar archivos de manera más libre, es por esto que no tienen control del tráfico ni de los archivos que se comparten y es por intermedio de estas comunicaciones que un atacante puede acceder al equipo de cómputo o puede compartir archivos que tengan malware que busca que le asignen permisos para poder acceder al control del equipo de cómputo o hasta a la manipulación de la misma, por ejemplo las redes más conocidas son uTorrent, Ares, Vuze, eMule.

De acuerdo con lo anterior, se debe tener en cuenta que se deben establecer mecanismos por medio de los cuales se puede mitigar el riesgo, dado que todo es responsabilidad del administrador y en algunos casos de los usuarios.

[10] Qué es un RootKit. https://www.avast.com/es-es/c-rootkit
[11] ¿Qué es p2p?. https://diccionarioactual.com/p2p/

Se debe tener claro que para que un bot o robot inicie su ataque y posterior administración del equipo de cómputo, se le debieron asignar permisos con privilegios, para esto, si el usuario lo ejecuta (programa o apertura del archivo) el con esa tarea ya se instalará y puede que en ese mismo momento ya este asociado a una botnet. Es por esto que los atacantes lo que hacen por lo general es camuflar los bots en archivos potencialmente deseables para la víctima, de manera tal que la misma de manera ingenua lo abrirá o ejecutará y se infectará de manera silenciosa, esto se puede ver en las páginas web o hasta en los correos electrónicos. Puede que los ataques no sean directos, también pueden ser enviados cuando se inyecta código en páginas web, ya que aprovechando la vulnerabilidad que pueda tener, lo pueden ejecutar en segundo plano esperando a que la víctima seleccione alguna opción especifica o hasta con un mensaje emergente y al momento que el usuario de clic se instale o ejecute.

Después de ejecutada la acción esperado, el bot es instalado y a continuación instala o ejecuta los métodos push style y C&C (comando y control) y en IRC (Internet Relay Chat o Charla en Tiempo Real), ya que los equipos de cómputo afectados están listas en cualquier momento, es así como el botmaster tiene a su disposición los equipos infectados, los cuales ya en ese momento son conocido como zombis y es entonces cuando solo con la ejecución de ciertos códigos, puede hacer que su botnet actué de manera masiva por ejemplo para atacar algún servidor, en este caso una denegación de servicios, distribución de malware, etc.

En la actualidad, se puede ver que la tecnología ya es tan portable que casi todo el mundo está utilizándola y están conectados casi todo el tiempo, esto se ve con el uso de los smartphone y las tablets; como en todos los casos, siempre es recomendable mantener actualizado el software e instalar solo aplicaciones oficiales, pero existen personas que se encargan de modificar las roms ofreciendo otras mal conocidas como cocinadas, las cuales al ser modificadas, les quitan programas que “no son necesarios” y así serán más rápidas y livianas, puede que en algunos casos esto sea cierto, pero en otros casos se trata de modificaciones realizadas por delincuentes y mediante las cuales instalan malware para atacar. De la misma manera se puede ver cuando instalan aplicaciones que no están avaladas por los markets oficiales, para estos casos la función de esas tiendas oficiales es la de evaluar y avalar las aplicaciones y aunque se puede decir que pueden pasarse aplicaciones, por lo menos si disminuye bastante el riesgo que puede correrse al instalar aplicaciones “piratas o no oficiales”. En el caso de los dispositivos móviles, se pueden evidenciar aún más las vulnerabilidades, ya que como son tan funcionales, suelen instalarse muchas aplicaciones a las cuales se les asignan permisos casi de todo el dispositivo, en muchos casos acceden a datos confidenciales como credenciales de bancos o para autenticación por ejemplo de correos, es por esto que si un dispositivo de este tipo es infectado, fácilmente acceden a toda esa información y pueden realizar muchos delitos, tanto así que se han conocido casos en los cuales proceden a clonar los equipos en estos casos es que toman el IMEI y lo asignan a otro dispositivo.

Finalmente, los ciberdelincuentes al acceder a los dispositivos móviles, pueden tener a la mano la información utilizada en la banca móvil, dado que los bancos hacen uso de las tecnologías cuando es posible, y esto en la actualidad es posible, dado que se pueden realizar transacciones desde los smartphones con solo tener instaladas las aplicaciones para este tipo de transacciones, es por esa razón que para los delincuentes es tan atractivo el buscar el acceso a los mismos, ya que allí se puede acceder a distintas credenciales para acceder a información personal, es por esto que es necesario el proteger no solo los equipos de mesa o portátiles, sino todos los dispositivos que puedan ser atacados y que tengan información sensible o personal.

6.3 MARCO CONCEPTUAL

Para el desarrollo del presente proyecto se deben tener claros unos conceptos básicos para un mejor entendimiento, los cuales se citan a continuación:

CIBERATAQUE: Son las acciones que se realizan con el fin de causar un daño a un sistema o la manipulación del mismo, esto se puede realizar a través de una serie de técnicas como por ejemplo mediante el uso de virus informáticos, correos no deseados, suplantación de identidad, uso de malware, ataques dirigidos para llegar a una denegación de servicios a través de envío masivo de solicitudes a un servidor

para que de esta manera se caiga el servicio, interferencia de las comunicaciones, etc[12].

CIBERDEFENSA: Trata de la aplicación e implementación de medidas de seguridad que se garantice y proteja la infraestructura de la información y las comunicaciones frente a los posibles ciberataques, está relacionado con la defensa digital, de los datos y la información[13].

SEGURIDAD INFORMÁTICA: Es la relación que se tiene entre la seguridad de la información y la protección de los datos, para garantizar esta seguridad, se debe garantizar que se cumplan los 3 pilares principales de la seguridad informática, los cuales son la confidencialidad, integridad y disponibilidad[14].

Confidencialidad: Acceso autenticado y controlado.

Integridad: Datos completos y no modificados.

Disponibilidad: Acceso garantizado

[12] Ciberataques, la mayor amenaza actual http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO09-2015_AmenazaCiberataques_Fco.Uruena.pdf

[13] Ciberseguridad y ciberdefensa: dos tendencias emergentes en un contexto global. http://52.0.140.184/typo43/fileadmin/Revista_119/Editorial.pdf

[14] Definición se Seguridad Informática. https://protejete.wordpress.com/gdr_principal/definicion_si/

Teniendo claro que es necesario establecer estos pilares para un óptimo manejo de la información y la gestión de los datos, también es recomendable que se tenga el control relacionado con la gestión de la misma, es por esto que tanto en el hogar como en las organizaciones es importante generar la conciencia relacionada con la importancia de la información.

Cuando se habla de la seguridad de la información, se hace referencia a los datos mismos donde lo que se busca es evitar la pérdida y/o la modificación de estos de manera no autorizada y es en este último punto es donde se habla de la autenticidad.

Por otra parte, cuando se habla de protección de datos, se puede hablar que es más la parte legal y es en este punto se busca la protección de los derechos personales de los individuos para evitar consecuencias negativas en contra de ellos

SOFTWARE MALICIOSO: Es conocido también como el software que es creado con la finalidad de afectar el comportamiento de los equipos de cómputo en los que se instala, por lo general este tipo de programas son divulgados en páginas que no gozan de buena reputación y que los mismos por lo general están vinculados con publicidad engañosa en donde por lo general dice que es un programa reconocido pero que se ofrece de manera gratuita, pero que al interior del mismo tiene otros programas que lo que hacen es buscar que le asignen permisos administrativos para poder ejecutar los mismos para vulnerar el sistema y apropiarse del mismo

para que realice actividades que no son asignadas por el propietario del equipo de cómputo[15].

ANTIVIRUS: Son programas que fueron creados con el fin de detectar y eliminar malware, esto en consecuencia a que con las mejoras tecnológicas, los ciberdelincuentes han detectado que pueden realizar actos ilícitos por intermedio de esos medios y es por esto que se crea la necesidad de crear herramientas mediante las cuales se pueda proteger la información y los dispositivos, y es por esto que existen diferentes tipos de antivirus como los siguientes[16]:

Antivirus Preventores[17]: Son lo que se encargan como su nombre lo dice, de prevenir al usuario antes que se presente la infección o instalación del malware.

Antivirus identificadores[18]: Es el encargado de identificar los virus que puedan estar atacando el equipo de cómputo e identifican programas que tengan códigos específicos relacionados con esos virus.

[15] Software Malicioso. https://www.consumidor.ftc.gov/articulos/s0011-software-malicioso

[16] Que es un virus informático. https://www.gcfaprendelibre.org/tecnologia/curso/virus_informaticos_y_antivirus/los_virus_informaticos/1.do

[17] Antivirus preventores. http://informaticaseguridaddiazpech.blogspot.com/2016/11/antivirus-preventores.html

[18] Antivirus Identificadores. http://virusinformaticosyantivirus.blogspot.com/2013/08/antivirus-identificadores-esta-clase-de.html

Antivirus descontaminadores[19]: Son aquellos que después de identificar el virus, se encarga de descontaminar el archivo o en su defecto de eliminarlo para de esta manera evitar que haga algún tipo de daño al sistema, en caso de haber detectado la contaminación, realiza la limpieza e intenta reestablecer el sistema al estado que se encontraba antes de ser infectado..

ANTIMALWARE: Se encarga de prevenir la instalación de malware (software malicioso); existen algunos que no solo prestan ese servicio, sino que adicionalmente pueden gestionar el control parental o administradores de contraseñas[20].

ANTISPAM: Software que identifica correo basura o no deseados, el cual elimina para de esta manera evitar que los buzones de correo electrónico se saturen, también elimina los mensajes sospechosos.

IDS O SISTEMAS DE DETECCION DE INTRUSOS: Son utilizados para detectar e acceso no autorizado bien sea a una red o a un computador, estos suelen hacer rastreos al tráfico de la red y de esta manera evitar ataques o informar si se está realizando una actividad sospechosa y de esta manera también evitar falsas alarmas[21].

[19] Resumen de antivirus http://serranop4030.blogspot.com/2012/11/resumen-de-antivirus.html
[20] Que es un antimalware. http://www.mejor-antivirus.es/preguntas/antimalware.html
[21] Detección de Intrusos en Timepo Real. https://www.segu-info.com.ar/proteccion/deteccion.htm

IPS O SISTEMAS DE PREVENCIÓN DE INTRUSOS: Sirve para controlar el acceso a la red y de esta manera evita los ataques que se puedan presentar. Al ser un control adicional de acceso, se comportaría similar a un cortafuego[22].

6.4 MARCO LEGAL

Para el desarrollo de este trabajo, se tendrá en cuenta la normatividad vigente en Colombia por medio de la cual se establecen las obligaciones que se deben tener como referentes para evitar la violación de algunos de esos lineamientos y con esto al igual que con las buenas prácticas adoptadas pretende tener el control de la información.

A continuación, se relaciona la normativa que aplica para este tipo de investigación con relación a los delitos que se pueden presentar:

LEY 527 DE 1999[23] - COMERCIO ELECTRÓNICO

[22] http://es.ccm.net/contents/163-sistema-de-prevencion-de-intrusiones-ips
[23] Ley 527 de 1999. http://www.mintic.gov.co/portal/604/w3-article-3679.html

Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones"

LEY 599 DE 2000[24]

Por la cual se expide el Código Penal. En esta se mantuvo la estructura del tipo penal de "violación ilícita de comunicaciones", se creó el bien jurídico de los derechos de autor y se incorporaron algunas conductas relacionadas indirectamente con el delito informático, tales como el ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas. Se tipificó el "Acceso abusivo a un sistema informático", así: "Art. 195. El que abusivamente se introduzca en un sistema informático protegido con medida de seguridad o se mantenga contra la voluntad de quien tiene derecho a excluirlo, incurrirá en multa."

LEY 962 DE 2005[25]

Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos. Prevé el

[24] Ley 599 de 2000. https://docs.supersalud.gov.co/PortalWeb/Juridica/Leyes/L0599_00.pdf
[25] Ley 962 de 2005. http://www.secretariasenado.gov.co/senado/basedoc/ley_0962_2005.htm

incentivo del uso de medios tecnológicos integrados para disminuir los tiempos y costos de realización de los trámites por parte de los administrados.

LEY 1150 DE 2007[26]

Por medio de la cual se introducen medidas para la eficiencia y la transparencia en la Ley 80 de 1993 y se dictan otras disposiciones generales sobre la contratación con Recursos Públicos. Específicamente, se establece la posibilidad de que la administración pública expida actos administrativos y documentos y haga notificaciones por medios electrónicos, para lo cual prevé el desarrollo del Sistema Electrónico para la Contratación Pública, Secop.

CIRCULAR 052 DE 2007[27] (Superintendencia Financiera de Colombia)

Fija los requerimientos mínimos de seguridad y calidad en el manejo de información a través de medios y canales de distribución de productos y servicios para clientes y usuarios.

LEY ESTATUTARIA 1266 DEL 31 DE DICIEMBRE DE 2008[28]

Por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la

[26] Ley 1150 de 2007. http://www.secretariasenado.gov.co/senado/basedoc/ley_1150_2007.html

[27] Circular 052 de 2007. https://www.superfinanciera.gov.co/jsp/loader.jsf?lServicio=Publicaciones&lTipo=publicaciones&lFuncion=loadContenidoPublicacion&id=20145

[28] Ley Estatutaria 1266 de 2008. http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html

financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones

LEY 1273 DEL 5 DE ENERO DE 2009[29]

Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Artículo 269[30]

LEY 1341 DE 2009[31]

Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la Información y las Comunicaciones –TIC, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.

RESOLUCIÓN DE LA COMISIÓN DE REGULACIÓN DE COMUNICACIONES 2258 DE 2009[32] Sobre seguridad de las redes de los proveedores de redes y servicios de telecomunicaciones. Esta resolución modifica los artículos 22 y 23 de la Resolución CRT 1732 de 2007 y los artículos 1,8 y 2,4 de la Resolución CRT 1740 de 2007.

[29] Ley 1273 de 2009. http://www.mintic.gov.co/portal/604/w3-article-3705.html
[30] Ley 1273 de 2009. http://acueductopopayan.com.co/wp-content/uploads/2012/08/ley-1273-2009.pdf
[31] Ley 1341 de 2009. http://www.mintic.gov.co/portal/604/w3-article-3707.html

[32] Resolución 2258 de 2009. http://itcomunicaciones.net/Resolucion%202258.pdf

Esta regulación establece la obligación para los proveedores de redes y/o servicios de telecomunicaciones que ofrezcan acceso a Internet de implementar modelos de seguridad, de acuerdo con las características y necesidades propias de su red, que contribuyan a mejorar la seguridad de sus redes de acceso, de acuerdo con los marcos de seguridad definidos por la UIT, cumpliendo los principios de confidencialidad de datos, integridad de datos y disponibilidad de los elementos de red, la información, los servicios y las aplicaciones, así como medidas para autenticación, acceso y no repudio. Así mismo, establece obligaciones a cumplir por parte de los proveedores de redes y servicios de telecomunicaciones relacionadas con la inviolabilidad de las comunicaciones y la seguridad de la información.

LEY 1453 DE 2011[33]

Por medio de la cual se reforma el código penal, el código de procedimiento penal, el código de infancia y adolescencia, las reglas sobre extinción de dominio y se dictan otras disposiciones en materia de seguridad. Artículo 8 Utilización ilícita de redes de comunicación.

NORMA ISO/IEC 27001:2013[34]

Estándar internacional que se aplica para la gestión de la seguridad de la información. Al manejar el Sistema de Gestión de Seguridad de la Información SIGI,

[33] Ley 1453 de 2011. http://www.mintic.gov.co/portal/604/articles-3709_documento.pdf
[34] Norma ISO 27001 https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001

se busca minimizar los riesgos, para esto se deben establecer procesos y procedimientos que ayuden a la organización a llegar a la excelencia.

7. DISEÑO METODOLÒGICO

7.1 TIPO DE INVESTIGACIÓN

El proyecto es una monografía de investigación, la cual se presentará desde un enfoque cualitativo, dado que se realizará desde el análisis de material bibliográfico que busca resolver la pregunta de investigación que se formuló.

Se realizará un análisis de los acontecimientos históricos presentados en relación con los ataques representativos y que en la mayoría de los casos están enmarcados en el marco de la ciberdelincuencia, para lo cual se aplicarán los conocimientos relacionados con la seguridad informática y la legislación que aplica para Colombia, es decir la ley 1273 de 2009.

7.2 DISEÑO DE INVESTIGACIÓN

Para el desarrollo del presente proyecto se recolectará la información la cual posteriormente se analizará para de esa manera tener todo el panorama del tema a tratar, esto enfocado al usuario final del equipo de cómputo y soportado en el marco de la ley colombiana (ley 1273 de 2009).

Por lo anterior, se utilizarán fuentes de información secundarias, esto como soporte bibliográfico, al igual que proyectos, tesis, artículos, conferencias o demás material que se encuentre relacionado con el tema para de esta manera poder hacer un mejor análisis.

Inicialmente se realizará el levantamiento de información relacionada con los ataques informáticos en la actualidad, a continuación, se procede a realizar el análisis de la misma para de esta manera poder identificar la importancia de la información y de los equipos de cómputo (pc) para de esta menara establecer las causas y consecuencias que se presentarían por la instalación de los botnets.

7.3 POBLACIÓN

Este proyecto está enfocado a los usuarios finales, personas que utilizan computadores (de escritorio y portátiles) a nivel personal, para generar conciencia sobre los mismos en relación a la importancia de proteger y adoptar buenas prácticas para el cuidado de la información y sus equipos de cómputo para que no se lleguen a ver en una situación incómoda como puede ser la perdida de información o en el peor de los escenarios en algún delito informático.

7.4 MUESTRA

Es cuantitativo, ya que, de acuerdo con la información recolectada de varias fuentes, se podrán identificar cuáles son las causas más comunes en este tipo de ataques, cuales son los patrones que más se repiten con relación a los tipos de ataques que realicen los ciberdelincuentes.

8. PRESUPUESTO

8.1 RECURSO HUMANO

Para el desarrollo del presente proyecto será necesario un ingeniero de sistemas quien realizará la investigación y que de acuerdo con sus conocimientos relacionados con la seguridad informática se enfocará en el desarrollo del problema planteado. Es así que debe realizar la tarea de búsqueda y organización de la información y posterior análisis para de esa manera obtener como resultado unas recomendaciones para dar cumplimiento al objetivo establecido en la presente investigación.

8.2 RECURSO TECNOLÓGICO

Los recursos tecnológicos utilizados en la presente monografía son los siguientes:

- Un computador de mesa, el cual tiene las siguientes características: Disco duro de 500 GB, Monitor LG de 21'', procesador Intel® Core™ i5 de 3.20 GHz, menoría RAM de 4.00 GB, Sistema operativo Windows 10 Pro de 64 bits.
- Internet banda ancha contratado con operador.
- Paquete ofimático Microsoft Office 2013.

8.3 RECURSOS FINANCIEROS

Los costos previstos para el desarrollo de la presente monografía son los necesarios en el tiempo estimado para la ejecución de la presente investigación, la cual se estima será en un semestre.

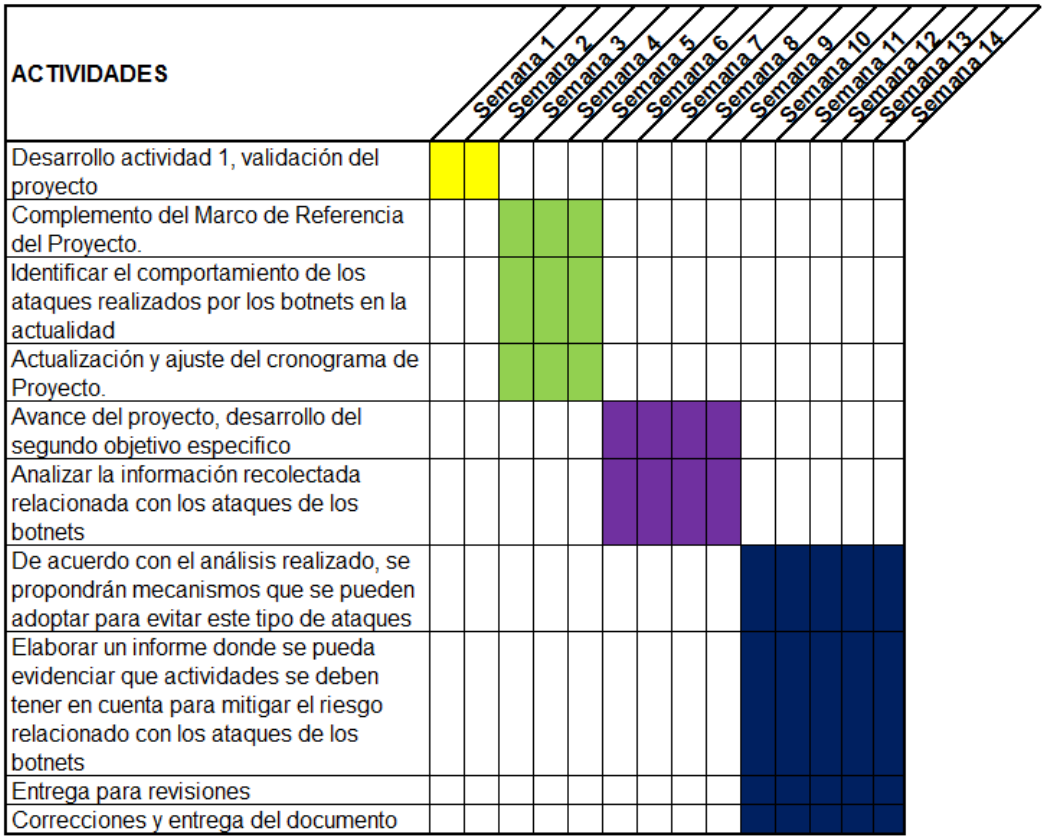
Tabla 1. Recursos Financieros

Ítem	Descripción	Valor mensual	Total (6 meses)
1	Servicio de Internet	$ 45.000	$ 270.000
2	Servicio de luz	$ 35.000	$ 210.000
3	Imprevistos		$ 50.000
Total			$ 530.000

Fuente: El autor.

Los gastos relacionados son los necesarios para el desarrollo del presente proyecto.

Ilustración 1. Cronograma de actividades

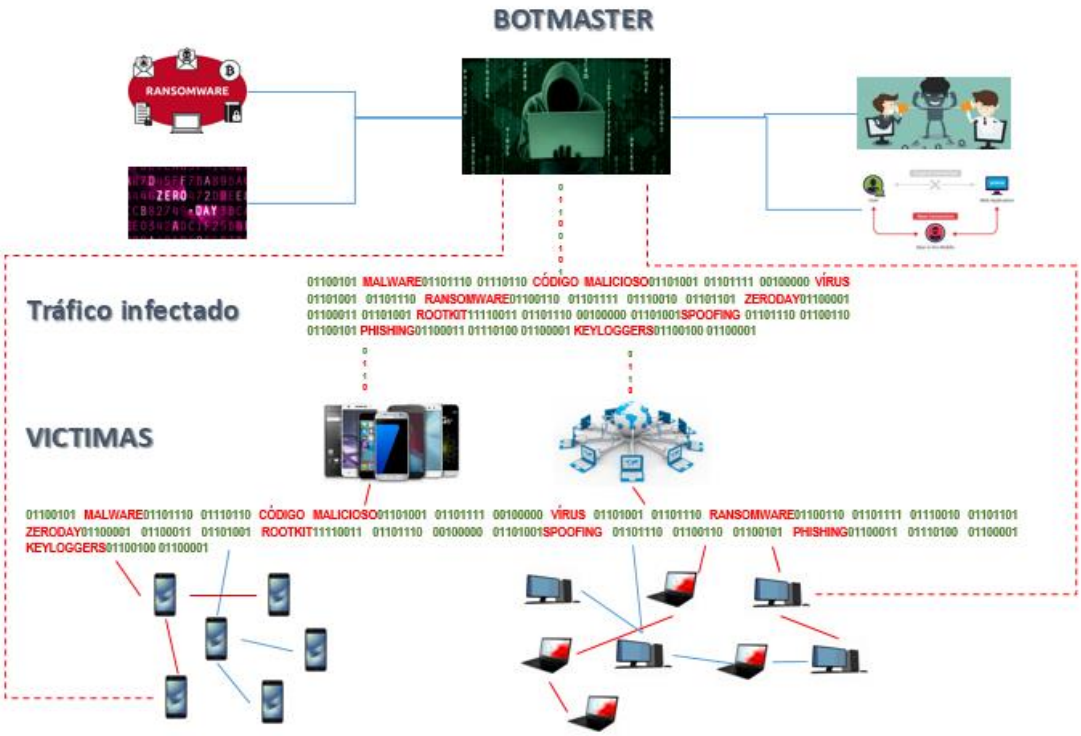


Fuente: El autor.

9. DESARROLLO DEL PROYECTO

En la actualidad, las tecnologías son utilizadas en muchas de las tareas que se realizan día a día, y es por esa razón que se ha convertido más que un lujo en una necesidad, por esa razón es que se puede acceder desde casi cualquier dispositivo a la información, dado que muchas de las actividades realizadas como trabajos, trámites, etc, están de alguna manera vinculadas por lo menos a una cuenta de correo electrónico o sistema de autenticación de alguna aplicación.

Ilustración 2. Arquitectura de una Botnet



Fuente: El autor.

De la misma manera, en la mayoría de las organizaciones se tienen establecidos programas o aplicaciones para la gestión de las tareas que realizan, para lo cual se deben tener establecidos parámetros y controles para el acceso a la información.

Por otra parte, en el ámbito personal, las personas se encuentran en un punto donde se encuentran conectados en todo momento, esto se refiere a qué gracias a las redes sociales, todos se encuentran interactuando en las mismas casi que de manera continua.

Teniendo en cuenta todo lo anterior, se puede ver que el uso de la tecnología es en este momento una herramienta necesaria, la cual ha pasado de un segundo plano en algo más prioritario; por ejemplo, las comunicaciones que se utilizaban de manera normal, más puntualmente refiriéndose a la vía telefónica, de correo físico y hasta el punto de la comunicación de manera presencial han sido remplazadas y/o optimizadas para una mejor gestión.

Este cambio conlleva a que toda la metodología relacionada con el comercio, se debe manejar de manera electrónica, razón por la cual se han detectado desde los inicios de las comunicaciones vía electrónica los ataques realizados por los ciberdelincuentes. Este componente se puede evidenciar con los correos electrónicos en la década de los 90, dado que se podía identificar que no se tenía clara la importancia de la información y los ataques que se podían realizar por ese medio.

La información siempre ha sido un insumo muy tentador para los delincuentes, dado que en el mercado negro es uno de los productos más cotizados, es por esto que los delincuentes se han dedicado a buscar las vulnerabilidades que se puedan identificar para de esa manera poder realizar los ataques y conseguir la información para el beneficio de ellos. Es por todo esto que se ha buscado la reglamentación para que se puedan castigar los actos ilícitos que se puedan presentar y de esta manera tener mayor control de la información y de los datos.

Los botnets[35] o redes de ordenadores, en la actualidad son utilizados por ciberdelincuentes, en estos casos son conocidos como botmaster[36]. Estos delincuentes se encarga de distribuir malware con el fin de infectar los equipos de cómputo para tenerlas a su servicio y poder realizar actividades ilícitas tales como ataques para denegación de servicios, envío de correos spam, robo de identidades, etc., y además son personas que están en busca de los ataques de día cero (en inglés 0-day), que son los fallo de seguridad no parcheados que afectan a la última versión del software que se quiera atacar, en los casos más conocidos se puede hablar de los productos Microsoft, es por esto que para estos productos se debe estar pendiente de las actualizaciones, dado que es cuando se detecta una vulnerabilidad de este tipo que se realiza un parche que corrija el error para evitar las vulnerabilidades a las que puede estar expuesto.

[35] Taller de Malwares #4 [Botnets]. http://www.antrax-labs.org/2011/12/taller-de-malwares-4-botnets.html
[36] http://www.eset-la.com/pdf/prensa/informe/tendencias_2011_las_botnet_y_el_malware_dinamico.pdf

Con el avance de la tecnología, y la adopción de la misma en el diario vivir, es posible encontrar en la actualidad que los dispositivos ya se pueden controlar de manera remota, esto se puede ver a gran escala en los edificios o casas inteligentes o en los automóviles que se puedes manejar sin estar en el interior del mismo, es por esto que aunque se facilitan algunas tareas, también se puede convertir en un arma de doble filo, razón por la cual se debe tener el control y mantener la seguridad en todo momento.

El objetivo de esta investigación es dar a conocer la importancia de la protección que se debe tener para la salvaguarda de la información, dado que todo lo que se usa por intermedio de la tecnología está conectado a la red y todo lo que se maneje por ese medio es susceptible a ser atacado bien sea de manera personal o específica, o por intermedio de ciberdelincuentes que utilizan sus conocimientos para automatizar estas labores y realizarlo de manera masiva, por esta razón se deben establecer y adoptar medidas de seguridad que ayuden a mitigar el riesgo y tener el control de los dispositivos.

9.1 ANÁLISIS DEL DESARROLLO DEL PROYECTO

Se puede encontrar que los ataques los aplican en cualquier escenario que se pueda, razón por la cual se deben tener buenas prácticas para la administración y manejo de las aplicaciones y la misma información. A continuación, se citan algunos de los casos en los cuales se pueden evidenciar los ataques:

En el acceso a internet, se pueden ver varios ataques por medio de los cuales los ciberdelincuentes buscan tener acceso a la información que se ingresa en los navegadores, es por esto que se puede presentar uno de los ataques conocidos como el hombre en el navegador[37] (man in the browser), estos ataques se pueden ver cuando se tienen certificados que han caducado o cuando se instalan certificados falsos, los cuales lo que hacen es que permiten la instalación de malware que utilizan para el robo de credenciales para el realizar transacciones no autorizadas o para la venta de las mismas.

Ilustración 3. Ataque hombre en el navegador (man in the browser)

Fuente: [Imagen de esquema ataque hombre en el navegador]. Recuperado de: http://secureonlinetransact.com/index.php?option=com_newsfeeds&view=category&id=17&Itemid=589

[37] Black Hat: cómo crear una botnet de 1.000.000 de navegadores. https://www.welivesecurity.com/la-es/2013/08/01/blackhat-como-crear-una-botnet-de-1-000-000-de-navegadores/

Otro tipo de ataque que se puede encontrar es en los casos que reciben correos electrónicos mediante los cuales ofrecen dinero o herencias, en esos casos los más inocentes caen en estas estafas dado que citan que ha sido ganador de una rifa y que para reclamarla debe enviar un dinero para que se pague el cargo del envío de la supuesta ganancia. En otro caso es cuando dice que una persona murió y que tenía una herencia, que para que no se pierda le envíen datos como la cuenta bancaria y otros datos para que se realice la transacción, pero con estos datos pueden realizar trámites como abrir cuentas bancarias, realizar compras por internet, etc.

Ilustración 4. Correos electrónicos falsos pidiendo información

Nuestra Referencia: CFG/MX/A001 — Entrada

De: Fundación Carlos Slim <dxorporat@kelantan.gov.my>
Asunto: **Nuestra Referencia: CFG/MX/A001**
Fecha: 22 de julio de 2010 9:40:23 GMT-05:00
Para: undisclosed-recipients:;
Responder a: carlosslim_grants@live.co.uk

Nuestra Referencia: CFG/MX/A001
Su Ref:

Attn Beneficiario,

La Fundación Carlos Slim se incorporó en 1986, con la misión de establecer una serie de proyectos sin fines de lucro, relacionados con la educación, la salud, la justicia y el desarrollo personal y colectivo, mediante la aportación de recursos humanos y económicos, para dotar a la sociedad mexicana de las herramientas necesarias para su superación profesional y social.
Los objetivos de la organización se han fortalecido y desarrollado con el tiempo, basado fundamentalmente en los principios de becas a los estudiantes de subvención, ayudas en efectivo a los profesionales, profesores y personas, para empezar, continuar y aplicar su aprendizaje a todos los ámbitos del conocimiento en usuarios domésticos y los centros internacionales de enseñanza superior, y también ayudan en la apertura, promover, fomentar, patrocinar, subvencionar, financiar y apoyar a los necesitados.
Nos complace informarle que como parte de nuestra promoción el año fiscal 2010, la Fundación Carlos Slim ha seleccionado a los beneficiarios para recibir la suma de dos millones de dólares EE.UU. en concepto de ayuda en efectivo.
Se requiere que usted nos envía la siguiente información, para el procesamiento y la documentación.

Nombres completos:
Género:
Fecha de nacimiento:
Dirección de contacto:
País:
Número de teléfono (s):
Ocupación:
Empresa:
Estado civil:

En nombre de la Fundación Carlos Slim, el Patronato, la amabilidad de aceptar nuestra felicitación.

Saludo atentamente,
Mr. Maurice Mercer
© 2010 Fundación Carlos Slim.
http://www.carlosslim.com

Fuente: [Imagen ejemplo de correo falso solicitando información]. Recuperado de http://www.dragonjar.org/me-gane-2-millones-de-dolares.xhtml

También se pueden encontrar ataques como los que envía por ejemplo de Microsoft mediante los cuales dicen que se encuentran en proceso de actualización de datos y que para eso debe ingresar nuevamente los datos en un link que dejan en el correo, en estos casos los usuarios están ingresando sus credenciales de manera transparente y de esta manera el atacante accede a los datos de manera limpia. En estos casos es ilógico que soliciten información de la cuenta teniendo, dado que para estos casos se realiza todo desde el mismo correo en sus opciones.

Ilustración 5. Estafa Lotería de Microsoft

Fuente: [Imagen de correo falso, suplantación a Microsoft, lotería de Bill Gates]. Recuperado de http://www.welivesecurity.com/la-es/2013/05/15/scam-doble-simula-provenir-microsoft-fundacion-bill-melinda-gates/

En el caso de los dispositivos móviles se puede presentar el tema de las vulnerabilidades relacionada con el software que no está validado por las tiendas de los sistemas operativos, en el caso de Android es el Play Store, dado que si se instalan aplicaciones que no han sido avaladas por estos markets, se puede estar instalando una aplicación falsa que lo que realiza es en primer plano unas tareas que pueden ser las que supuestamente ofrece, pero en un segundo plano puede estar corrompiendo los archivos, robando credenciales, enviando información personal, etc; otra vulnerabilidad que se puede presentar es cuando se instalan Roms cocinadas o modificadas para los móviles, en estos casos cuando se encuentran, citan que son más livianas y que desinstalaron programas que no se utilizaban para que el sistema sea más fluido, pero en estos casos si no se tiene conocimiento de lo que se está instalando, es preferible evitar este tipo de aplicaciones, dado que internamente puede estar conectando los dispositivos a una botnet para que puedan ser manipulados de manera remota o que no sean seguros los dispositivos.

Otro ataque que se puede encontrar es el Ransomware o secuestro del equipo de cómputo, el cual se identifica cuando mediante un malware se secuestra o tiene acceso a algún archivo y cuando se encuentra infectado no permite que se pueda manejar el mismo, de la misma manera puede secuestrar directamente el equipo de cómputo y el delincuente pide dinero para rescatar o recuperar el archivo o el equipo de cómputo. Este malware por lo general es propagado en correos electrónicos no solicitados, los cuales pueden ejecutarse cuando se descargan o ejecutan los

anexos, otra opción es cuando se accede a páginas que no son confiables, o se accede a una supuesta página oficial desde un link que envían, en este caso pueden tener acceso al equipo de cómputo y poder manipularla, en estos casos se puede ver cuando ejecuta otro programa para que se active la cámara del equipo y de esta manera trasmite lo que se está viendo en el momento y es de esta manera que las personas creen que alguien los está vigilando y es en ese momento donde los usuarios de manera ingenua caen en este tipo de ataque y acceden al pago del rescate; otro caso es cuando se habilita una pantalla supuestamente de un organismo de control como la policía donde intimidan dando información relacionada con los datos o el material encontrado como contenido pornográfico, evidencia de visita a esos sitios o que se tiene instalado software ilegal, razón por la cual le solicitan al usuario el pago de la multa. En la mayoría de los casos se puede encontrar este tipo de virus en páginas de contenido erótico, sexual, o de descarga de software ilegal.

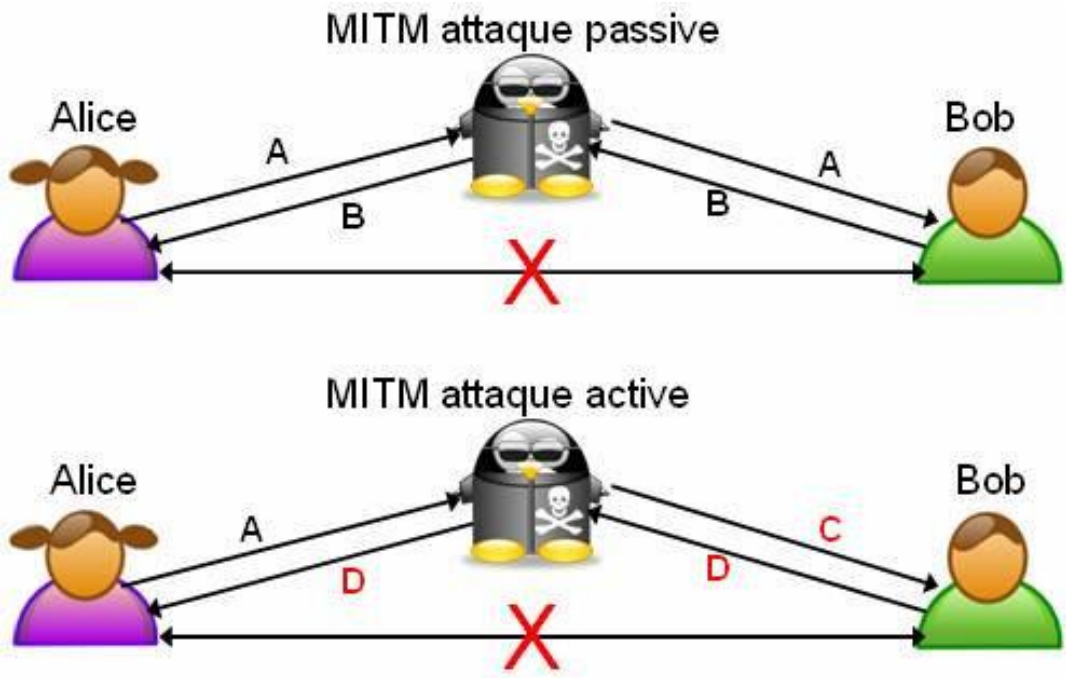
Ilustración 6. Ransomware

Fuente: [Imagen presentación de Ransomware cuando secuestra la máquina de la víctima]. Recuperado de https://www.welivesecurity.com/la-es/2018/05/29/formas-ransomware-puede-comportar-al-infectar-sistema/

Con el uso de los medios para la comunicación, también es muy común encontrar el tipo de ataque de hombre en el medio (man in the middle) que se trata de la interceptación de las comunicaciones, por ejemplo cuando se está diligenciando algún formulario web o se ingresan las credenciales para acceder a algún sitio, en este caso la información debe estar encriptada o con mecanismos de control para

que en el momento que se vaya a trasmitir, no sea transparente o clara para cualquier persona que pueda acceder a la misma, en estos casos se puede ver cuando el atacante se ubica en el puente o medio donde se realiza la comunicación y la intercepta de manera casi indetectable y puede ver todo lo que está transitando en ese momento, en este caso se puede acceder a las credenciales o datos personales de los usuarios. Este mismo ataque es muy claro cuando los usuarios se conectan a la redes wifi que estén abiertas, en estos casos la información puede ser fácilmente capturada por un delincuente.

Ilustración 7. Ataque hombre en el medio (man in the middle)



Fuente: [Imagen esquema ataque hombre en el medio]. Recuperado de https://inforensicsuex.wordpress.com/tag/man-in-the-middle/

Todo este tipo de ataques se ha manejado de manera “oculta” para los usuarios, esto se refiere a que gracias al desconocimiento de las medidas de seguridad, o a la falta de conciencia relacionada con la ejecución de archivos de dudosa procedencia o acceso a páginas con el mismo estilo o con contenido no debido, los ciberdelincuentes trabajan por esos medios donde cargan archivos o aplicaciones que se encargan de estos ataques, los cuales son más conocidos cómo virus, dentro de los cuales se encuentran los siguientes:

VIRUS INFORMATICO: Programa malicioso que al ser instalado realiza actividades para dañar el sistema o modificarlo, el cual puede auto ejecutarse y dependiendo de su programación, realizará diferentes tareas. A continuación se relacionan unos de los virus más conocidos[38]:

- Mydoom (W32.MyDoom@mm, Novarg, Mimail.R o Shimgapi
- CIH (Chernobyl o Spacefiller)
- Win32/Simile (Etap)
- Frethem
- Virus de macros
- Virus de sobre escritura
- Virus de Programa
- Virus de Boot

[38] (RIVERO, 2011). “¿QUÉ SON LOS VIRUS INFORMÁTICOS?”. {En línea}. {13 de Enero de 2011}. Disponible en internet: https://www.infospyware.com/articulos/%C2%BFque-son-los-virus-informaticos/

- Virus Residentes
- Virus de enlace o directorio
- Virus mutantes o polimórficos
- Virus falso o Hoax
- Virus Múltiples

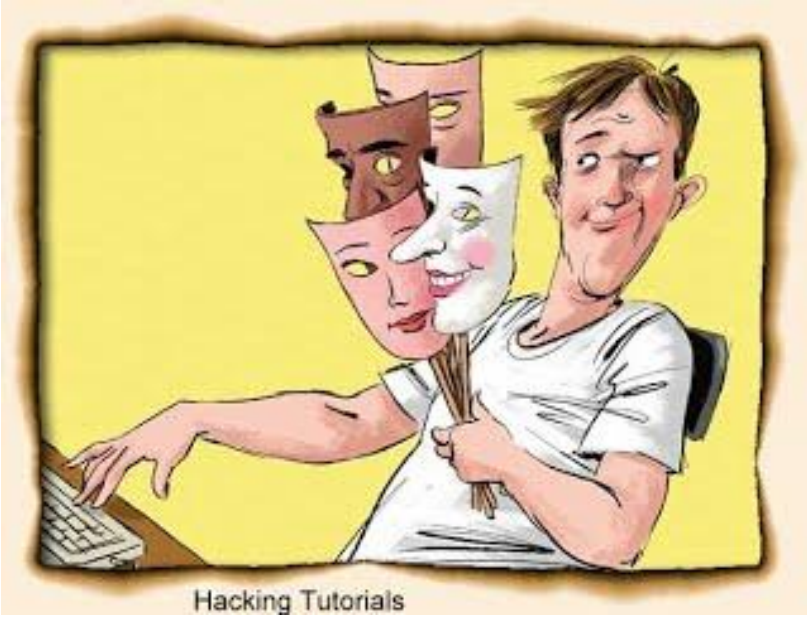
Ilustración 8. Vírus informático

Fuente: [Imagen afectación al ordenador si es infectado con un virus]. Recuperado de https://lasupergalaxia.wordpress.com/tag/gusano-informatico/

SPOOFING: Este tipo de ataque trata de la suplantación de identidad de un remitente de correo para acceder a la información. Esto se hace teniendo acceso a la ip de confianza, por el conocimiento del tráfico que se realiza en el envío de la

información o mediante la suplantación del host y la identificación de la ip para no levantar sospecha a la víctima[39].

Ilustración 9. Spoofing



Fuente: [Imagen ataque Spoofing o suplantación de identidad]. Recuperado de https://www.informatica-hoy.com.ar/software-seguridad-virus-antivirus/Spoofing-El-virus-que-envian-los-amigos.php

KEYLOGGERS: Programa que captura y graba lo que se pulsa en el teclado y posteriormente lo remite a la persona que lo haya instalado, mediante esta práctica el delincuente puede saber todo lo que realizó la víctima en el equipo de cómputo infectado.

[39] Hablemos de Spoofing. https://hacking-etico.com/2010/08/26/hablemos-de-spoofing/

Ilustración 10. Keyloggers

Fuente: [Imagen ejecución de un keylogger]. Recuperado de https://arstechnica.com/information-technology/2017/05/hp-laptops-covert-log-every-keystroke-researchers-warn/

TROYANOS (TROJAN): Es malware que se instala o guarda en los equipos y que están dentro de programas o archivos legítimos (software, música, fotos, correo electrónico) y su objetivo es crear puertas traseras (backdoor) para que el atacante pueda acceder al equipo de cómputo o administrarlo de manera remota, también es utilizado para el robo de credenciales. A continuación, se relacionan unos de los troyanos más conocidos:

- NetBus

- Back Oriffice 2000
- SubSeven
- Cybersensor
- DeepThroat v2
- Dolly Trojan
- Girlfriend 1.35
- InCommand v1.0
- NetSphere
- Master Angel 97

Ilustración 11. Troyanos (Trojan)

Fuente: [Imagen modelo de malware troyano]. Recuperado de http://ruberush.blogspot.com.co/p/virus-gusanos-y-troyanos-informaticos.html

ROOTKIT: Es una aplicación con una serie de programas que usa el atacante para que al instalarse manipule los procesos que ejecuta el equipo de cómputo para de esta manera camuflarse y no ser detectado y de esta manera poder realizar las actividades que le fueron programadas.

Ilustración 12. Rootkit

Fuente: [Imagen permisos asignados a un rootkit]. Recuperado de http://www.google.com.co/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&ved=0ahUKEwjhlqTX37fPAhWElB4KHYcFDYIQjRwIBw&url=http%3A%2F%2Fmauriciosandoval00.blogspot.com%2F2009%2F04%2Fconceptos-de-virus.html&psig=AFQjCNGAAvMWh2IeFeRapzlWj13lTUkuUQ&ust=1475347352246208&cad=rjt

GUSANO INFORMATICO: Malware que se propaga en el ordenador sin necesidad que el usuario interactúe con él, de la misma forma, tiene la facultad de replicarse y estos programas consumen mucha memoria, razón por la cual puede llegar a bloquear los servidores o los equipos de cómputo hasta llegar a dejarlo bloqueado. A continuación, se relacionan unos de los gusanos más conocidos:

- Host Computer Worm
- Network Worms
- Bubbleboy Worm
- I Love You
- Blaster (Lovsan o Lovesan)
- Sobig Worm

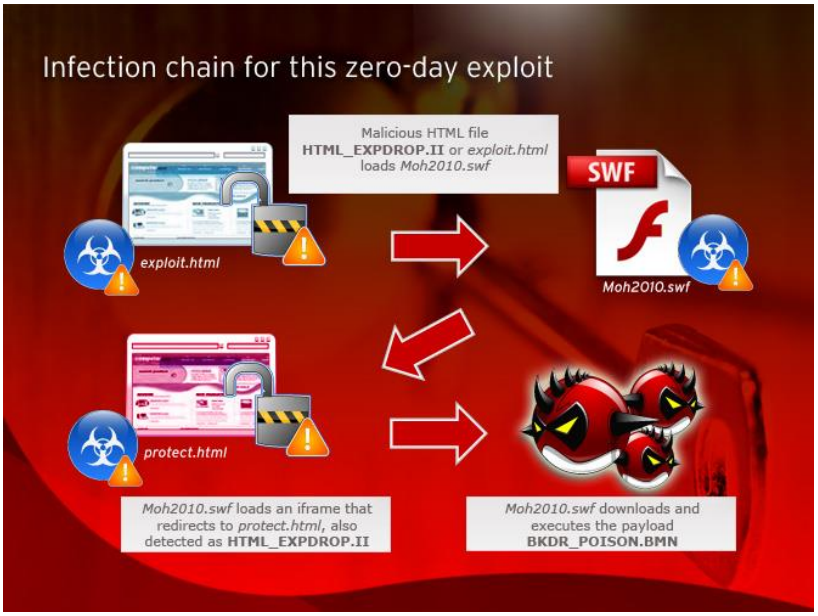
Ilustración 13. Gusano Informático

Fuente: [Imagen propagación o movimiento de un gusano Informatico]. Recuperado de http://www.definicionabc.com/tecnologia/gusano-informatico.php

EXPLOIT: Es un programa que ejecuta tareas para intentar aprovechas vulnerabilidades que pueda tener un sistema, con el fin de aprovecharlo y tener acceso al equipo de cómputo y poder manipularla a su antojo, también para el robo de información.

ZERO DAY: Es cuando se ha detectado un exploit y no se ha corregido, es cuando se aprovecha esa vulnerabilidad identificada que el usuario no ha corregido y por allí lo ataca.

Ilustración 14. Zero Day



Fuente: [Imagen modelo ataque zero day]. Recuperado de https://blog.hackersonlineclub.com/2016/01/silverlight-zero-day-exploit-hacking.html

PHISHING: Este ataque es más conocido sobre todo con páginas bancarias, el atacante crea una página web idéntica a la original, la victima al ver gráficamente que la página es válida, procede a ingresar sus credenciales para acceder al banco de manera virtual, y es allí donde el atacante cumple con su propósito. Para este caso es importante seguir las recomendaciones dadas por las mismas entidades bancarias para evitar estos casos.

Ilustración 15. Phishing

Fuente: [Imagen presentación phishing – pagina falsa]. Recuperado de https://www.spamloco.net/2012/01/phishing-te-ganaste-un-premio-formulario-adjunto.html

De acuerdo con lo anteriormente expuesto, vale precisar que en su gran mayoría los ataques o las infecciones son realizados como ataques web[40], los cuales son

[40] Ataques Web. http://www.ru.tic.unam.mx:8080/tic/bitstream/handle/123456789/1726/31.pdf?sequence=1&isAllowed=y

por lo general ejecutados porque el usuario no toma las debidas precauciones para la protección de la información, como por ejemplo validar las paginas en las que está navegando, validar que si se envía información sea de manera segura (cifrada), ingresando a lugares o sitios oficiales, no desde links que han sido enviados por correos electrónicos o dando clic en páginas de dudosa reputación o también descargando software ilegal.

9.1.1 Riesgos asociados a los botnets.

La información, los datos y hasta los equipos de cómputo, equipos (personales (pc o portátiles)) se encuentran expuestos a ataques constantemente, dado que la información ha recibido en los últimos tiempos mucho más valor que las aplicaciones o programas, es por esta razón que los ciberdelincuentes se han especializado en realizar ataques dedicados a ubicar y explotar las posibles vulnerabilidades que pueda tener, en algunos casos son vulnerabilidades de las aplicaciones o los sistemas operativos, es en estos casos cuando el usuario no sigue las recomendaciones dadas, tales como mantener los sistemas y aplicaciones actualizados, ya que como son publicadas las posibles vulnerabilidades y los respectivos parches o actualizaciones para corregir esas fallas o posibles accesos que pueden utilizar para los ataques, esos casos son conocidos como zero day, los cuales al ser detectados y estudiados, pueden llegar a dejar el equipo de cómputo con puertas o accesos mediante los cuales pueden atacar y llegar a tener el control parcial o total y de esta manera utilizar los recursos para el beneficio de los delincuentes.

Es de anotar que la información siempre va a ser importante, aunque parezca que no lo es, dado que existen personas que la utilizan para su beneficio, se puede hablar por ejemplo de los trabajos que puedan encontrar en equipo de cómputo, la música, las fotos, los registros, hasta los contactos que se tengan en algún archivo, esto se puede utilizar de diferentes maneras, por ejemplo para suplantar la identidad de una persona para de esta manera acceder a otros datos, o para delinquir en casos como delitos informáticos conocidos como estafa, secuestro de información, venta de servicios que se supone que son legales pero solo buscan el beneficio del delincuente, creación de falsos perfiles para de esta manera realizar otro tipo de delitos, etc.

Por otra parte, los ciberdelincuentes buscan la información de las empresas u organizaciones para venderla a personas que buscan reputación en internet, posibles vínculos para negocios o en el peor de los casos el daño a la víctima como por ejemplo publicar información que se supone que es privada para de esta manera pierdan credibilidad y lleguen hasta al cierre de las mismas o para que la competencia pueda tener los datos de sus clientes y así ofrecer productos o servicios y así de manera desleal hacer que la competencia salga del mercado, esto es visto como un delito.

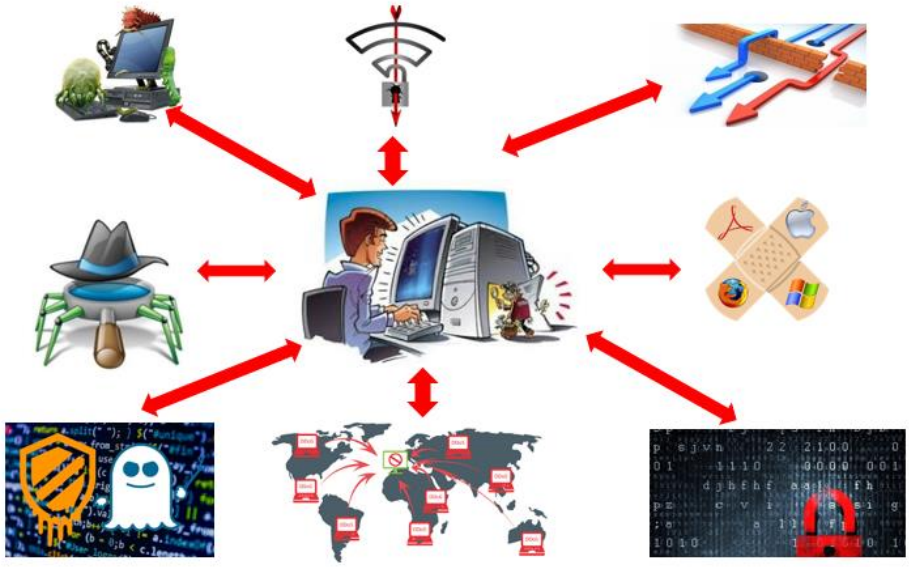
Los ataques[41] mencionados y los riesgos asociados a los mismos son solo una parte, ya que los ciberdelincuentes al tener un conocimiento mucho mayor que el de la mayoría de los usuarios, buscan no solo extraer la información que tengan almacenada, sino que también buscan tener el control de los equipos de cómputo para de esta manera poder esos recursos a su disposición y de esa manera poder delinquir de manera masiva y sin ser detectados fácilmente; este caso es cuando los equipos de cómputo o dispositivos caen en alguno de esos ataques y el delincuente puede llegar a la manipulación del dispositivo, es aquí cuando el equipo de cómputo puede ser capturado y se puede decir que se convierte en un bot (robot), en estos casos el delincuente (bootmaster) tiene una red en la cual va agregando los equipos de cómputo que ataca y de esta manera puede manipularlas para realizar los ataques de manera más controlada; uno de los ataque más conocidos por estos delincuentes es el de envío de correo malicioso (spam), es cuando al acceder a las cuentas y tomar datos de directorios (lista de correos electrónicos), envía correos a esos destinatarios para que esa potencial victima al ver que es una cuenta conocida, acceda al contenido y allí pueda a través de diferentes técnicas, pueda hacer que caiga en sus ataques y así lo pueda unir a su botnet para continuar con los ataques.

Teniendo claros los riesgos a los que se encuentran expuestos, ahora es necesario entrar en materia con lo relacionado a los ataques propios de las botnets, que para

[41] Qué es una botnet o una red zombi de ordenadores. https://www.osi.es/es/actualidad/blog/2014/03/14/que-es-una-botnet-o-una-red-zombi-de-ordenadores

ser más exactos están relacionados con el robo de identidad y de credenciales para de esta manera realizar las actividades ilícitas. En su gran mayoría, los atacantes o ciberdelincuentes realizan los ataques de una manera sencilla, crean programas mediante los cuales al ser ejecutados en los equipos de cómputo de las víctimas las infectan y en ese momento tienen acceso a las mismas, se descarga un software dañino el cual al instalarse convierte al equipo de cómputo atacado en un bot o robot, ya en ese momento la victima estará dentro de una botnet la cual a su vez está vinculada y puede ser manipulada por el botmaster; Es en este momento que de manera remota tendrá el control de los dispositivos conectados en la botnet para realizar las actividades en busca de su beneficio. Estos ataques suelen presentarse cuando los usuarios acceden a páginas de dudosa reputación, ya que los delincuentes en las páginas cargan programas o realizan ataques buscando vulnerabilidades que puedan tener los usuarios y por ese medio buscar el acceso no autorizado. Estas redes zombi son muy apetecidas por muchos usuarios dado que gracias a las mismas se pueden realizar ataques o tareas de manera masiva, los botmaster pueden acceder a la información almacenada o tratada en los bots y esta información son las credenciales, cuentas de correo, las listas de contactos, información personal o empresarial y la información bancaria y con esta información pueden realizar ataques masivos a páginas web, enviar publicidad no deseada, correos spam o realizar compras no autorizadas por internet.

Ilustración 16. Tipos de ataques asociados a las Botnets



Fuente: El autor.

A continuación, se citarán con más detalle los ataques a los que se encuentra expuesto si es convertido en un bot:

ROBO DE INFORMACIÓN: En este caso, el botmaster puede acceder a la información de los usuarios que tengan información almacenada o registrada en el bot, la información más deseada son los datos personales ya que si la tiene puede llegar a realizar una suplantación de identidad y realizar actividades ilícitas, números de tarjetas de crédito para realizar compras por internet, credenciales bancarias para hacer transacciones y cualquier otra información que le pueda servir como por ejemplo información empresarial o familiar.

PROPAGACIÓN DE INFORMACIÓN: Se presenta cuando tienen acceso a correos electrónicos mediante los cuales pueden realizar envíos masivos de información dado que pueden acceder también a las listas de contactos y enviar correos no deseados o spam, de la misma manera al enviar correos a personas que estén en la lista de contactos, quienes reciben la información al ver que es de un contacto conocido no dudaran en abrir los correos mediante los cuales también pueden enviar virus, software malicioso para también convertir a esos destinatarios en nuevos bots o instalación de software espía.

FRAUDE MEDIANTE CLICS: En este caso específico es cuando las personas buscan tener buena reputación en alguna página, o para aumentar la facturación de publicidad web.

DENEGACIÓN DE SERVICIOS: Para estos ataques, los botmaster hacen que su botnet realice peticiones de manera masiva a un servicio o servidor, con esto buscan dejar fuera de línea el servicio dado que por la cantidad de peticiones saturan el servidor, esto por lo general se ve en páginas web.

Cabe anotar que las botnets como se ha citado a lo largo de este documento, son equipos (personales (pc o portátiles)) zombis que trabajan como marionetas, dado que se ejecutan en conjunto cuando el botmaster les envía la orden para hacer ataques dirigidos de manera controlada, pero adicionalmente a esto, existen unas que utilizan la red de manera legal para propagarse y contaminar de manera más

efectiva y evitando su detección, ese es el caso de eDonkey y Torrent, ya que son botnets parásitas; se identifican de esa manera dado que no existen mecanismos de defensa contra las mismas o como hace unos años se veía también con el programa Ares, ya que al ofrecer descarga de programas de manera gratuita y eficaz, le solicitaba al usuario que desactivara cualquier tipo de protección como el firewall o el antivirus y adicionalmente permisos para acceder a los archivos, de esta manera la información se encontraba vulnerable y podía ser compartida sin ninguna restricción y por esa misma razón al realizar búsqueda de algún tipo de archivo, programa, video, etc, así mismo se descargaba cualquier cantidad de malware.

Las botnes están compuestas por un cliente-servidor, la manera más común es cuando el atacante realiza una suplantación de identidad y envía algún archivo como por ejemplo una foto o algo llamativo para la víctima, la cual de manera inocente procede a ejecutar el archivo y de esa manera le permite el acceso al ciberdelincuente en el caso que se está tocando sería el botmaster cuando por ese método envía el bot para que se instale en el equipo de cómputo de la víctima y convertirlo en un zombi. En la actualidad se puede ver ese tipo de ataques cuando por medio de las redes sociales utilizan publicidad que llame la atención o crean perfiles falsos que llamen la atención para que los usuarios accedan y ejecuten alguna tarea para que así pueda acceder el bot a las terminales y poder infectarlas, pero no solo se ve en esos casos, también se puede ver cuando solicita actualizaciones de programas, en la mayoría de los casos se puede evidenciar con las actualizaciones de java, que en muchos casos lo que hacen los atacantes es

enviar un programa que al ejecutarse abre una pantalla que dice que es necesaria una actualización y para ello le pide que le asigne permisos o solicita la clave de administrador, es allí cuando si el usuario no tiene claro estos tipos de actualización ,puede caer y dar pie a que se instale el malware para que accedan a su equipo de cómputo.

Las botnes a lo largo de su historia han sido creadas para construir servidores para alojar software, cracks, seriales, etc., también para alojar material pornográfico, para crear servidores por medio de los cuales se puedan realizar ataques tipo phishing, para intercambios de material ilegal, robo de información y credenciales, manipulación de juegos online, distribución e instalación de malware y ataques de denegación de servicios.

La función más conocida de las botnets[42] o la más usada es la denegación de servicios distribuida[43] (DDos) es en teoría la misma de una denegación de servicios, solo que en este caso se usan muchos equipos de cómputo de manera simultánea, ya que de esa manera pueden hacer que el servidor u objetivo quede fuera de servicio de manera más efectiva.

[42] Cómo combatir una botnet y entender su impacto real https://www.welivesecurity.com/la-es/2014/10/27/botnets-como-combatirlas/

[43] Ataque de denegación de servicio (DDoS). https://searchdatacenter.techtarget.com/es/definicion/Ataque-de-denegacion-de-servicio

Los bots están programados de manera tal que sean casi imposible detectarlos, ya que por lo general son transportados en la red de manera normal, si levantar ninguna sospecha, y por esto pueden ingresar por los puertos que son usados comúnmente; adicional a eso, al mantener el mecanismo de comando y control, pueden actualizarse cuando lo deseen y así pueden hacerse invisibles a los antivirus. Los bots también están programados con algunos exploits, los cuales al ejecutarse en los equipos de cómputo víctimas, si las mismas no están protegidas de manera debida o actualizada, pueden hacer mucho daño al equipo zombi.

Uno de los casos más conocidos en este tipo de redes es la botnet Zeus[44], la cual cuenta con un módulo por medio del cual el botmaster puede monitorear y ver en tiempo real como está actuando la red y que tareas están ejecutando los zombis, en este caso se ve expuesta la confidencialidad de la información de cada una de las víctimas. A partir de esa botnet se creó otra conocida como Kneber, la cual según informes en el año 2007 tenía reclutadas aproximadamente 75.000 zombis. Esto es bastante preocupante, dado que lleva a la conclusión que no se tienen buenas prácticas para la protección de la información o de sus equipos de cómputo, e indica que no se establecen mecanismos de seguridad que protejan de manera eficiente, y no solo eso, sino que también se detecta que no se tiene una cultura organizacional y personal enfocada a la seguridad de la información y una concientización sobre la protección de la información.

[44] ZeuS Botnet y su poder de reclutamiento zombi. http://mipistus.blogspot.com/2009/10/zeus-botnet-y-su-poder-de-reclutamiento.html

Es importante conocer la familia de los botnet las cuales se citan a continuación:

Agobot: Bot que está disponible en la red, creada bajo licencia GPL, escrito en lenguaje C++ y por esa razón que es multiplataforma.

SDbot: Malware más activo en el momento, creado en lenguaje C bajo licencia GPL también disponible en internet.

GTBot: Amenaza Global, usado con IRC, protocolo utilizado para mantener conversaciones en tiempo real y esta opción la aprovecha usando una instancia IRC invisible para el usuario y por ese medio añade características por medio de scripts con extensión ".mrc" los cuales son usados para controlar el bot.

DSNX: Escritos en lenguaje C++ bajo licencia GPL, permite que el atacante extienda y las funcionalidades del bot y pueden realizar ataques DDoS escaneo de puertos)

Q8 Bots: Escrito en lenguaje C creado para sistemas Unix/Linux.

Kaiten: Escrito para Linux/Unix y aprovecha la vulnerabilidad del usuario en la autenticación y de esta manera secuestra fácilmente el equipo de cómputo.

A continuación, se relacionan las causas, problemas y respectivos efectos que conlleva la falta de mecanismos de seguridad y posibles infecciones o instalaciones de malware en los equipos de cómputo:

Las causas más significativas como se ha hablado en el presente documento, es la instalación o uso de código malicioso por medio del cual se expone la integridad y protección de los sistemas, también esto va de la mano con la instalación de software pirata, antivirus conseguidos en sitios de dudosa reputación como por ejemplo en páginas poco confiables, la no actualización de los mismos o del software y finalmente el acceso a usuarios no autorizados o el no control de la administración de los equipos de cómputo, ya que por esa razón pueden instalar software pirata.

El problema que se puede presentar es que la información almacenada en las estaciones de trabajo se verá desprotegidas de cierta manera y es en esos casos que los ciberdelincuentes pueden acceder a la misma y al control de los equipos de cómputo para realizar actividades ilícitas (delitos informáticos).

Finalmente, los efectos que conlleva este tipo de vulnerabilidades son la propagación de malware, inestabilidad de la red e inseguridad en los sistemas. Con la inestabilidad tanto de la red, como de los mismos sistemas, puede dar paso a la instalación de los bots para de esa manera convertir los equipos de cómputo en zombis y así mismo como se instalan en algunos terminales, se propagará el

malware a todos los equipos de cómputo que se encuentren en la red o con las que tenga algún tipo de comunicación. Así mismo, la instalación de software pirata lo que hace en muchos de los casos es abrir puertas traseras para que los ciberdelincuentes puedan acceder a los equipos de cómputo, y en el caso de los antivirus que no son licenciados, no garantizan la seguridad necesaria para la protección de los sistemas o de la misma red.

En muchos de los casos, se puede ver que el software gratuito lo que hace es que se ejecuta de manera limpia para el usuario, pero en un segundo plano puede estar afectando el equipo de cómputo con un malware, como por ejemplo corrompiendo los archivos o registros del sistema, creando puertas traseras, enviando información a algún delincuente, el cual ha modificado el ejecutable e insertado código que lo que hace es enviarle información para que él se beneficie.

Es por esa razón que es importante establecer mecanismos de seguridad, política que salvaguarden la información y protejan los equipos de cómputo, implementar medidas que permitan proteger la información y las comunicaciones, como por ejemplo sistemas de encriptación, políticas de seguridad, restricción a la información, roles para la gestión de la información y la seguridad, mantener la seguridad de la información, backups, tener actualizado el software, desinstalar los programas que no sean necesarios u obsoletos, crear reglas para el tráfico de la red, cerrar los puertos que no se están utilizando, y dado el caso establecer un protocolo para cuando se habiliten.

Así las cosas, la integridad de los equipos que estén infectados con algún malware o como un zombi en una botnet, se encuentra expuesta toda la información que se tenga almacenada, al igual que las credenciales de los usuarios, datos de correos electrónicos, cuentas de redes sociales, cuentas bancarias, cuentas de servicios, información que se tenga almacenada, el uso de la red donde se está conectada la víctima, pueden secuestrar el equipo o dispositivo por medio de un ransomware donde el ciberdelincuente cifra la información de manera tal que no se pueda acceder a la misma, y la única manera de recuperar la información es pagando lo que pida el ciberdelincuente como rescate de la misma. Después que la máquina se encuentre infectada el ciberdelincuente puede realizar diferentes tipos de delitos, como por ejemplo enviar más malware a los contactos de la víctima, envío de spam, usar los recursos de la máquina víctima para su beneficio, realizar delitos suplantando la identidad de la víctima, injuria o calumnia en redes sociales y como se ha visto en los últimos tiempos la sextorsión (uso de fotos o videos que encuentra en el ordenador y que amenaza con la divulgación de ese material a sus contactos y/o la publicación del mismo en la red).

El comportamiento de las botnet es así: El botmaster o creador de la botnet se encarga de distribuir un virus o malware de diversas formas como por ejemplo con la ingeniería social para saber cuáles son las vulnerabilidades que pueden haber y que los usuarios en medio de su ingenuidad caen en esos ataques; otra manera es infectar las páginas de dudosa reputación ya que cuando las víctimas ingresan a las mismas no saben al riesgo al que se encuentran expuestos; otra es cuando acceden

a links que envían por correo electrónico, ya que de esa manera al ingresar se infectan sin darse cuenta, en esos casos es cuando se infecta la máquina pero es transparente para la víctima; otra forma es cuando abren archivos de remitentes que no conocen, por lo general en esos archivos se ejecutan los ataques para que los ciberdelincuentes puedan tener acceso a las máquinas; otra modalidad es cuando llegan correos de “las entidades bancarias” donde indican que deben acceder para algún trámite como actualización de contraseñas, beneficios por productos, etc; también existen otros ataques que se pueden ejecutar cuando se conectan dispositivos a los equipos de cómputo, por lo general son dispositivos usb que se encuentran por ahí tirados y los usuarios no tienen la precaución de validar que puede ser un dispositivo infectado, en este caso como en los casos de dispositivos conocidos siempre se debe realizar previamente un escaneo para validar que no se encuentre infectado, ya que como se ha citado anteriormente, el ataque se realiza y la víctima no se da cuenta ya que son procesos que se ejecutan en segundo plano y por lo mismo no van a ser evidentes para el usuario final; otro de los ataques muy conocidos es cuando se instala, ejecuta o descarga software de sitios de dudosa reputación o que al momento de la instalación solicitan permisos de administrador para realizar cambios en los registros del sistema que por lo general se pueden identificar como programas para craquear licencias, esto debido a que en su ejecución acceden como se citó al registro del sistema y desde allí modifica el mismo y de esa manera evade controles como validación de licencias, esto es un peligro dado que así como realiza su función, también deshabilita o da permisos al software para que permita acceder a permisos de administrador,

permisos por medio de los cuales puede cambiar la configuración que se tenga y así poder deshabilitar puertos o controles para que vulnere la seguridad de los equipos y puedan acceder los atacantes, en estos casos es cuando por ejemplo se puede convertir la máquina en un bot e integrarlo a una botnet para posteriormente realizar cualquier tipo de ataque o delito informático.

Es así como un conjunto de programas se ejecuta de forma automática y que permiten controlar los ordenadores o servidores infectados de forma remota ya que son parte de una botnet.

En la actualidad los sistemas operativos de Microsoft son los más susceptibles a ser atacados, dado que son los más comerciales a nivel mundial, es por ello que los hackers[45] en su constante búsqueda de encontrar vulnerabilidades de los sistemas, encuentran los fallos o posibles vulnerabilidades de los sistemas para de esta manera fortalecer los mismos, en esta tarea al encontrar alguna de esas vulnerabilidades, se reporta en diversos sitios, y es en ese momento cuando se hacen los respectivos ajustes para mitigar esos riesgos, es conocido como los service pack o parches de seguridad, para el caso de Microsoft, ellos cargan esos parches para que en el momento que los equipos se conecten y busquen actualizaciones, descarguen el parche y así poder garantizar la seguridad a los usuarios. Como esa información es reportada, los ciberdelincuentes pueden

[45] http://dle.rae.es/?id=JxlUKkm

identificar esos fallos y es cuando aprovechan los mismos para realizar sus ataques; pero no solo lo hacen por ese medio, también lo pueden realizar a través del protocolo de red telnet, accediendo de forma remota y aprovechando sus falencias de seguridad ya que la información viaja sin ningún tipo de cifrado y así intentar convertir las máquinas a las que está accediendo en zombis para que hagan parte de su botnet.

Si el ciberdelincuente logra infectar el equipo de cómputo, lo vincula a su botnet y entonces el botmaster puede controlar la máquina de forma remota, accediendo así a la totalidad de la información que se encuentre allí almacenada y con la misma poder usarla para su beneficio que en la mayoría de los casos es en delitos informáticos, como suplantación de identidad, compras no autorizadas, venta de la información o los datos al igual que de las fotos que pueda tener, al igual que por ejemplo un ataque de denegación de servicios distribuidos a páginas web causando en la misma el error 503 (servicio no disponible) en este caso es cuando el servidor no puede procesar una solicitud debido a la saturación de solicitudes, envío de spam, virus, software espía, etc., también el fraude por clics ya que a ellos les pagan por cada clic, entonces ordenan a los bots que tengan en su red a realizar esa tarea, también la minería y robo de bitcoints (criptomoneda). Una manera de identificar si se está infectado bien sea por un malware o que se encuentre en una botnet es cuando el rendimiento del equipo de cómputo se ralentiza, cuando la conexión a internet no es la óptima (uso injustificado del ancho de banda), que se muestren mensajes misteriosos o que por ejemplo alguno de sus contactos le notifique sobre

un correo, el cual el usuario nunca envió. En todos los posibles escenarios, el equipo de cómputo no estará utilizando sus recursos en lo que el usuario los tiene destinados, sino que por el contrario, se verá comprometido ese rendimiento, ya que al estar en una botnet, el botmaster tendrá la máquina en su poder, usando esos recursos para su beneficio y en cualquier momento usar esa botnet para ataques específicos, es por ello que en muchas ocasiones los usuarios al no tener la prevención o precaución para la seguridad de sus equipos, son infectados y comprometidos tanto en recursos como en la información que tengan almacenada y sus datos personales.

9.1.2 Peores Botnets de la última década.

A continuación se citarán en orden cronológico las botnets más conocidas en la última década:

Rustock[46]: Al parecer fue creado en diciembre del 2006 pero fue detectado por los antivirus y software de malware hasta el año 2007, de naturaleza tipo troyano, esto dado que se camuflaba en los archivos adjuntos de los correos y tipo spammer, esta botnet cuando estaba activa podía enviar hasta hasta 20.000 correos basura por

[46] Todo sobre el rootkit Rustock. https://securelist.lat/todo-sobre-el-rootkit-rustock/67338/

hora, infectaba a las víctimas y enviaba los correos, los cuales parecían que eran legítimos, es por esa razón que los correos no detectaban el correo spam.

Storm[47]: Del año 2007, de naturaleza gusano informático, principalmente se encargaba de recolectar direcciones de email para envío de correos spam y ataques de denegación de servicios (DDoS), para ser propagado, los ciberdelincuentes infectaban los archivos que estaban cargados en sitios web de descarga populares, de esta manera las víctimas descargaban los archivos y se infectaban de manera silenciosa, también se veía comprometido el rendimiento de la máquina dado que era utilizado en la mayoría de los casos para realizar ataques de denegación de servicios.

Cutwail[48]: Del año 2007, esta botnet tipo spammer con datos estadístico en el año 2010 con el envío de 74 millones de correos spam al día en el año 2010 y también utilizada para ataques de denegación de servicios.

Grum[49]: Del año 2008, especializado en el envío de correo spam, basado en mover los servidores de comando y control a nuevas ubicaciones; pese a que se desactivó

[47] Enciclopedía de Vírus, https://www.pandasecurity.com/peru/homeusers/security-info/40877/Storm.worm

[48] Botnets y sus efectos: un breve repaso a alguna de las más destacadas, https://blogs.protegerse.com/2015/03/02/botnets-y-sus-efectos-un-breve-repaso-a-alguna-de-las-mas-destacadas/

[49] Lo que debes saber sobre Grum y Botnet Takedown, https://es.computer-clans.com/what-you-should-know-about-grum-and-botnet-takedown

en el año 2012, es recomendable en todos los casos tener un buen software de antivirus y actualizado, ya que en su época tuvo gran éxito porque los usuarios no tenían el software adecuado para poder evitar ese tipo de ataques.

Coficker[50]: Del año 2008, se propago como malware tipo gusano que estaba enfocado en ataques a los sistemas operativos de Windows y después de encontrarse en la máquina de la víctima, se podía controlar de manera remota por el botmaster, utilizaba una vulnerabilidad en el servicio de Windows server o a través de dispositivos extraíbles como USBs. Dado que su ataque estaba enfocado a sistemas Microsoft, los administradores liberaron actualizaciones para dar solución a la vulnerabilidad, es por esto que siempre se recomienda que se tenga actualizado el software, dado que con las actualizaciones se da solución a las vulnerabilidades identificadas.

Kraken[51]: Del año 2008, de tipo spammer, teniendo como novedad que podía evadir el antimalware y con la capacidad de realizar auto actualización; ello era una desventaja dado que si los ciberdelincuentes querían ejecutar alguna nueva tarea, lo podrán hacer por ese medio.

[50] Botnet: Conficker, https://www.osi.es/es/servicio-antibotnet/info/conficker

[51] El ataque de los Botnets, https://www.danysoft.com/los-12-peores-botnets/

Mariposa[52]**:** Creado en el año 2008 pero descubierto hasta el 2009 creado en España, esta botnet a diferencia de las anteriormente mencionadas es de naturaleza Keylogger, ello para robar datos personales, credenciales, cuentas bancarias, contraseñas, etc., los creadores de esta red trabajaban con servicio de encriptación para de esa manera evitar ser detectado por los antivirus y su conexión era a través de redes virtuales privadas anónimas para el manejo de la botnet, de esa manera era muy difícil identificar la IP real. Esta botnet se utilizó para cyber-estafa y ataques de denegación de servicios.

Kelihos[53]**:** Del año 2010, de origen ruso, esta botnet utilizaba la comunicación tipo P2P y dado ello era muy difícil su detección; afectó es su mayoría los sistemas Windows, sus ataques eran spammer, de denegación de servicios y para la minería de datos (robo de Bitcoins o para generar ese tipo de moneda), podía propagarse a través de sitios de dudosa reputación, a través de links, correo spam, medios externos contaminados, documentos y a través de Facebook.

ZeroAccess[54]**:** Del año 2011, troyano especializado en atacar sistemas Windows, con la estructura de un Rootkit, que ofrece servicios como activación se productos, generador de claves para activar software, que afectaba a la víctima haciendo cosas

[52] Red de Bots Mariposa, https://www.pandasecurity.com/spain/mediacenter/malware/red-de-bots-mariposa/

[53] Botnet: Kelihos, https://www.osi.es/es/servicio-antibotnet/info/kelihos

[54] La Botnet ZeroAccess, http://www.mejor-antivirus.es/noticias/la-botnet-zeroaccess.html

como deshabilitar el antivirus, el firewall de Windows y por su naturaleza troyana se podía camuflar para no ser detectado, adicionalmente habilitaba puertas traseras y de esa manera poder manejar la máquina de manera remota, para realizar delitos informáticos tales como realizar estafas para conseguir bitcoins o beneficiarse en campañas de pago por click.

Gameover Zeus[55]: Creado en Rusia en el año 2012, su manejo era de comando central y control de redes y comunicación P2P para que fuera mucho más difícil de desarticular. Afectó los sistemas Microsoft, capturando las credenciales y contraseñas de los usuarios que ingresaban en los sistemas que ya estaban infectados, utilizando la inyección de código en los procesos del sistema o en los navegadores para almacenarlo en su panel de control para luego darle uso para ataques como envío de correo spam, campaña pagos por clic y ataques de denegación de servicios; adicionalmente esta botnet también infectaba a sus víctimas cuando descargaba mucho más malware, llegando hasta a la instalación de Cryptolocker (Ransomware), con ello lograba secuestrar la máquina de la víctima encriptando toda la información y de esta manera pidiendo dinero para el rescate de la misma, ello sin garantizar que fuera recuperada o simplemente teniendo el control para poder volver a secuestrar la máquina y continuar con la extorsión.

[55] ¿Qué es GameOver Zeus y por qué seguiremos viendo nuevas variantes?, https://www.welivesecurity.com/la-es/2014/07/22/que-es-gameover-zeus-por-que-seguiremos-viendo-nuevas-variantes/

Este último es uno de los más actuales ataques y peligrosos dado que el ransomware o secuestro ha sido de los ataques más preocupantes, ya que a pesar de todo lo citado, muchos de los usuarios aún no le dan la importancia que merece la seguridad de la información, y solo cuando están en el rol de víctimas es que comienzan a tomar conciencia, ya que el pensamiento general es que para nadie es importante la información que tengo, pero no saben que con solo un poco de información pueden llegar a utilizarla hasta para cometer delitos informáticos, es por ello que se trata no solo de tener software, sino que ya se profundiza más en la conciencia que se debe tener con la información y no solo en cuanto a software sino que también con el hardware.

Analizando los ataques realizado por las botnets más conocidas, se puede concluir que por medio de propagación del malware y haciendo uso de las vulnerabilidades identificadas en el software, los ciberdelincuentes realizan ataques que tienen éxito, dado que los usuarios no son conscientes de la importancia de la información y los mismos sistemas, esto dado que no utilizan software actualizado o simplemente no actualizan con los parches que ayudan a solucionar las vulnerabilidades identificadas y de esa manera mitigar el riesgo de convertirse en una víctima o bot; de la misma forma, se puede concluir que las botnet a pesar que pueden ser utilizadas para realizar diferentes actos ilícitos, en su gran mayoría son utilizados para uso de spammer y ataques dirigidos para denegación de servicios (DDoS).

Para concluir, es recomendable utilizar software confiable, mantenerlo actualizado, no tener instalado software que no se necesite o que sea de dudosa procedencia, dado que puede estar infectado con algún tipo de malware o puede tener vulnerabilidades que pueden afectar el buen funcionamiento del dispositivo o equipo de cómputo, al igual que se recomienda tener instalado software para mitigar el riesgo, tal como antivirus, antimalware, antispam, firewall y se recomienda para el caso del hardware que se configure de acuerdo con las necesidades del usuario, ya que muchos de los dispositivos como por ejemplo un modem tienen configuraciones estándar, las cuales pueden ser modificadas por los ciberdelincuentes, quienes realizan un estudio detallado de todas las posibles vulnerabilidades que puedan existir para realizar sus ataques.

Finalmente se puede concluir que la mayoría de los ataques están enfocados en los sistemas de Microsoft, no quiere decir que sean los más vulnerables, sino que son los más comerciales, pero esto no quiere decir que los otros sistemas como IOS o Linux no sean vulnerables, sino que no son tan comerciales como los de Microsoft, es por esto que la recomendación general siempre va a ser la misma, que en lo posible se utilice la versión más recientes del software y no dejar las configuraciones de fábrica para así mitigar el riesgo de ser una víctima de los ciberdelincuentes.

10. GUÍA DE RECOMENDACIONES PARA TENER EN CUENTA CON EL FIN DE MITIGAR EL RIESGO Y EVITAR SER PARTE DE UNA BOTNET O DE SER PARTE DE UN DELITO INFORMÁTICO RECOMENDACIONES

Se debe tener en cuenta que las aplicaciones están creadas para lo que fueron hechas, esto quiere decir que las medidas que se deben implementar son diversas, no se puede dejar la seguridad de la información solo en una medida de seguridad, para ser más claro, para estar protegidos de los ciberataques no es posible solo con un software, se debe partir desde la conciencia del usuario, que sepa a lo que se encuentra expuesto en la actualidad, que tengan conciencia del valor de la información y de los dispositivos que maneja, llámense portátiles, equipos de escritorio, smartphones, etc, luego se deben establecer medidas de seguridad que se citaran a continuación:

- Tener conciencia que todos estamos expuestos a ser atacados, ya que toda la información que tenemos puede ser utilizada para muchas cosas.

- Capacitar y concientizar a las personas sobre la importancia de la seguridad de la información.

- Instalar antivirus de casas de software reconocidas o de buena reputación como por ejemplo Symantec, Eset, Panda, Avast, AVG, etc., de igual manera se recomienda que se mantenga actualizado y con escaneo en línea, ya que si llegan

a detectar alguna vulnerabilidad, publicarán la solución para mitigar el riesgo al que se pueda ver expuesto el usuario final.

- Instalar antivirus con capacidad proactiva que permita detectar archivos maliciosos como Eset NOD32, Eset Smart Security con protección contra Botnets, Panda Gold Protección, Avast – antiphishing.

- Si es posible, usar un WAF (Cortafuegos de aplicaciones web), ya que con ese dispositivo se puede hacer el análisis del tráfico web entre el servidor e internet, esto quiere decir la conexión entre el usuario final desde cualquier dispositivo e internet.

- Instalar herramientas y productos antimalware.

- Mantener actualizado el software, ya que así se puede mitigar el riesgo asociado a vulnerabilidades que se puedan encontrar en el mismo.

- Solo instalar el software necesario.

- No ingresar a páginas web de dudosa reputación.

- No ingresar a páginas donde pidan credenciales como usuario, contraseña, pin, etc., desde links, mejor ir directamente a la barra de direcciones y digitar la url a la que se desea acceder.

- Si es necesario acceder desde un link, siempre validar que la dirección esté bien escrita, dado que si tiene una letra mal o no está completa, se puede estar accediendo a una página clonada en este caso sería un phishing donde al verse como la página original los usuarios digitan la información y es allí donde están entregando todos los datos a los ciberdelincuentes.

- Validar que en la página que se está accediendo tiene el protocolo de seguridad (https:// y un candado cerrado) ya que eso garantiza que la información que se está digitando se enviará cifrada, con ello si algún ciberdelincuente realiza un ataque de hombre en medio no podrá ver la información enviada.

- Mantener los navegadores actualizados y no instalar plugins sobre el mismo que no se necesiten, dado que por ese medio también pueden los ciberdelincuentes acceder a la información registrada.

- Tener una solución de seguridad con firewall para poder tener controlar las comunicaciones del equipo con internet

- Descargar software desde los repositorios oficiales, analizar previamente el software antes de la instalación y validando que sea la versión más reciente ya que tendrá resueltas las vulnerabilidades encontradas y corregidos los errores de código que se hubieran detectado.

- Utilizar un sistema operativo con soporte, esto quiere decir que se puedan realizar actualizaciones para corregir las vulnerabilidades encontradas para evitar los zero days o exploits.

- Generar contraseñas robustas, por ejemplo que tengan más de 8 caracteres, que tenga mayúsculas, minúsculas, números y caracteres especiales, esto dificulta que si están mirando lo que se está digitando, sea más complejo el identificarla.

- Evitar contraseñas fáciles de identificar tales como nombres de hijos, padres, etc, la mascota o cosas así, ya que uno de los ataques que realizan los delincuentes es la ingeniería social y por ese medio pueden tener fácilmente esos datos, al igual que no dejar de manera pública la información personal, dado que así también pueden realizar análisis y poder tener varias opciones para intentar identificar la posible contraseña, esto teniendo en cuenta que otro ataque que pueden realizar es el de fuerza bruta, esto quiere decir que los delincuentes con la información recopilada pueden hacer un listado de posibles contraseñas y realizar el ataque con la información recopilada hasta poder identificar la contraseña.

- No dejar generar contraseñas fáciles de identificar como por ejemplo teclas seguidas o solo numéricas, aunque no es la solución de fondo, por lo menos si es más complicado para el atacante identificar la contraseña, es recomendable implementar un segundo factor de autenticación para así tener mayor seguridad como lo es la aplicación latch, la cual permite bloquear las cuentas que se tengan configuradas para que no se pueda acceder a las mismas sino hasta cuando se active el pestillo.

- Existen exploits para activar los dispositivos como por ejemplo la cámara web de los computadores y así pueden grabar todo lo que está haciendo el usuario, es recomendable tapar las cámaras o desactivarlas con el fin de evitar ser espiados.

- No utilizar el usuario administrador para el uso de los equipos de cómputo solo para lo necesario, en lo posible generar un usuario que no tenga los permisos de administración ya que si se es atacado, no tendrá los privilegios para poder hacer modificaciones.

- Para los usuarios de sistemas Microsoft, existe una herramienta gratuita llamada Microsoft Baseline Security Analyze, la cual realiza análisis y evaluación de vulnerabilidades del sistema operativo, se recomienda el uso de esta herramienta dado que trabaja igual que las actualizaciones automáticas y de esa manera si llega a identificar vulnerabilidades las informa y así se puede tener la información para actualizar a todos los usuarios para minimizar los riesgos que se logren identificar y

así poder fortificar la seguridad del sistema operativo. (Esto para usuarios de versiones Windows Server 2008 R2, Windows 8.1, Windows 7, Windows Server 2008, Windows Vista).

- Realizar las descargas de actualizaciones desde los sitios oficiales, no desde sitios de dudosa reputación, ya que si se hace desde la segunda es un potencial riesgo de infección o ataque por parte de los ciberdelincuentes.

- Deshabilitar la ejecución automática de los dispositivos USB, ya que pueden haber malware que se ejecuta desde el mismo momento que se ejecuta el dispositivo y al estar de manera automática no se podrá identificar de manera oportuna ese tipo de ataque.

- Cuando se reciban mensajes por correo electrónico, evitar los que sean de remitentes no conocidos, en caso de abrirse el correo, si tiene archivos adjuntos o enlaces a otros sitios, evitar ejecutar los archivos al igual que validar las extensiones de los mismos y no acceder a los links ya que si se ejecuta el archivo puede tener algún malware o en el caso del link puede que filtre de igual manera software malicioso, en el caso de los hipervínculos en la mayoría de los casos los usuarios esperan que se abra otra ventana direccionando a un sitio, pero puede ser un ataque que solo necesita que se dé clic sobre el link y ya, de esa manera ya se puede estar infectado.

- Evitar la publicación de las direcciones de correo electrónico en sitios de dudosa reputación, dado que pueden haber ciberdelincuentes que capturan las mismas para el envío de correo spam.

- Implementar el uso de filtros anti-spam para evitar el correo no deseado, al igual que evitar responder ese tipo de correos ya que puede ser un parámetro que manejen para validar las cuentas de correo activas.

- Procurar no acceder a WiFi de sitios desconocidos, ya que se corre el riesgo que exista algún delincuente que intente capturar la información que se transmite al estar conectado a la red; si es necesario usar una red WiFi de un sitio no conocido se recomienda utilizar una VPN (Red Virtual Privada).

- Cuando se vaya a acceder a algún portal bancario, se recomienda no acceder desde links que sean enviados, es mejor digitar la dirección para de esa manera validar que se está ingresando al sitio deseado.

- Se recomienda usar software legal, ya que cuando se descarga o adquiere de sitios de dudosa reputación puede ser que sea software adulterado, esto con la finalidad de desactivar los parámetros de seguridad y de la misma manera dejar puertas traseras para que los ciberdelincuentes puedan realizar sus ataques.

- Procurar no acceder a páginas donde se deban ingresar credenciales desde sitios públicos como bibliotecas o café internet, dado que pueden estar infectados con malware o configurados con programas como los que detectan todo lo que se digita en los computadores. Si es necesario utilizar internet desde ese tipo de sitios se recomienda borrar los archivos temporales, cache, cookies, direcciones URL y contraseñas de los navegadores que se hayan utilizado.

- No reutilizar contraseñas para varios sitios, al igual que generar contraseñas complejas.

- Realizar copias de seguridad periódicamente, dado que si se llega a caer en algún ataque como un rasomware lo recomendable es no pagar lo que piden para recuperar la información.

- Realizar periódicamente escaneo de vulnerabilidades en los equipos de cómputo con el software instalado.

- Para los casos de uso de hardware como por ejemplo el router, se recomienda cambiar la contraseña que lleva por defecto.

- No ejecutar programas que piden quitar permisos como el del firewall, antivirus, etc.

- En caso de no poder pagar una solución, se pueden usar herramientas gratuitas de las casas de software, las cuales ofrecen servicios básicos para la protección de los sistemas, por ejemplo Análisis del pc gratis con Panda Could Cleaner, Avast – antimalware gratuito.

- Se recomienda establecer controles que permitan la protección de los datos, en el caso de las organizaciones, que se establezcan parámetros o buenas prácticas que contribuyan con la protección y conservación de los mismos.

- Implementar una política de seguridad que permita blindar la infraestructura de la organización y salvaguardar la información.

- Ante cualquier actividad sospechosa se debe actuar de manera preventiva, y establecer mecanismos para prevenir los riesgos que puedan presentarse.

- Se deben establecer medidas que permitan asegurar la información, tales como la encriptación de la información, crear contraseñas seguras y en lo posible con métodos de autenticación que aseguren el acceso a las aplicaciones.

- No utilizar la misma contraseña para todos los sitios.

- No ingresar a páginas desde enlaces que lleguen en correos electrónicos, es mejor acceder directamente a la página, ya que al momento de dar clic se puede

está accediendo a otro sitio, o se puede ejecutar alguna instrucción que no es visible para el usuario final.

- No ingresar a páginas de dudosa reputación, no instalar software que no sea confiable, administrar las aplicaciones y la red de manera responsable para salvaguardar la información y la integridad de los equipos de cómputo.

- En el caso de los dispositivos móviles, instalar antivirus, ya que los ciberdelincuentes también atacan ese tipo de dispositivos dado que en la actualidad tenemos mucha información en los mismos y son elementos muy vulnerables y apetecibles para ser atacados.

- En caso de descarga de software libre hacerlo desde sitios de confianza y siempre teniendo en ejecución la consola de antivirus, ya que es por esas páginas que muchas veces los ciberdelincuentes realizan los ataques.

- Al ingresar a páginas en internet validar que tengan protocolo de seguridad de transferencia (https), esto dado que los datos se cifrarán al momento de su trasmisión y si llegase a haber un ataque como por ejemplo el del hombre en medio, no podrán visualizar la información registrada, mientras que si se hace desde una página sin este protocolo (http), toda la información en el proceso de envío de información, se cargarán en un archivo plano, el cual tendrá toda la información

registrada (en este caso pueden tener todos los datos como usuario, contraseña, datos personales, números de cuenta, etc).

10.1 Como evitar ataques de phishing.

Como primera medida se debe identificar un correo Phishing y de esa manera eliminarlo sin realizar ninguna otra acción con el fin de mitigar el riesgo asociado a ese tipo de ataque, para ello se citan a continuación algunas pautas a tener en cuenta:

- Verificar el origen del correo (persona natural o jurídica), con esto si es de alguna entidad y no se tiene conocimiento de la misma, se puede descartar, si es de persona natural y casualmente es de origen de algún contacto conocido, lo mejor es en lo posible preguntar antes de abrirlo, esto teniendo en cuenta que puede ser una suplantación de identidad y al abrir el correo puede descargarse algún malware que contamine la máquina.

- No ingresar a los links que lleguen en un email, con esta medida se puede evitar una infección o secuestro de la máquina, ya que al darse clic en los links que llegan pueden en segundo plano ejecutar tareas que no puede percibir el usuario o puede cargar algún formulario que puede parecer el real, pero en verdad lo que hace es capturar la información que se ingresa en el mismo para posteriormente realizar algún acto ilícito.

- Se debe tener algún antivirus instalado, en lo posible con herramientas anti-spam, anti-phishing y antimalware para que pueda identificar una posible amenaza, igualmente se debe mantener actualizado el software, ya que las casas de ese software cuando identifican amenazas realizan las acciones correctivas y de esa manera se mitigan los riesgos que puedan presentarse.

- En el caso de necesitar ingresar datos personales o que puedan ser producto para un delito informático, se debe validar siempre en la barra de direcciones que se esté utilizando el protocolo de envío cifrado de los datos, esto se identifica en la barra de direcciones donde aparezca la dirección debe estar al inicio un candadito cerrado y enseguida https:// y la dirección de la página donde se está navegando.

- Activar notificaciones automáticas de acciones realizadas en las cuentas, por ejemplo cuando se accede al email, que se notifique que se está ingresando, esto con el fin de identificar de manera inmediata si accedieron a la cuenta o si intentaron el acceso a la misma. En este caso si se identifica que están intentando ingresar, la recomendación es cambiar de inmediato la contraseña.

- Se debe tener claro que el phising no solo lo realizan en páginas de entidades bancarias, también en redes sociales o e-comerce, ya que al tener acceso a esas cuentas, los ciberdelincuentes pueden cometer diversos delitos como por ejemplo extorsión, suplantación, robo de datos, robo de información, transacciones ilícitas, etc.

- Validar la dirección de la página web, por lo general puede estar mal escrita (puede que les falte una letra, que esté mal escrito, que tenga una letra cruzada, que tenga mala ortografía), o el dominio no coincide, por ejemplo que deba ser .gov y diga .com.

- Validar el idioma de la página, que todo el contenido de la misma esté en el idioma que está trabajando y validar que todo esté bien escrito, que no tenga faltas de ortografía.

- En caso de identificar alguna actividad irregular, se debe dar aviso a la entidad bancaria, puede ser por llamadas extrañas o ante cualquier correo sospechoso.

- No suministrar información personal mediante correo electrónico si no se tiene certeza del mismo, tener cuidado con la información que se suministra, por lo general son páginas supuestamente de entidades bancarias las que envían correos solicitando información personal. Cabe tener en cuenta que muchas entidades bancarias evitan solicitar información por ese medio ya que es de esa manera que los ciberdelincuentes en medio de la ingenuidad de los usuarios solicitan información y ellos al ver algún logo o dominio de la entidad, dan por válida la solicitud de la información.

- Usar filtro anti-spam, en el caso de los navegadores existen varios plugins que se encargan de identificar ese tipo de correos y los filtran para que no los vea el usuario y así evitar que los usuarios accedan a esos correos.

- Evitar el autocompletado en los navegadores, ya que si se ingresa en una página falsa, se cargaran automáticamente los datos almacenados, en cambio sí se digitan las contraseñas cada vez que sea necesario, se puede evitar ese tipo de ataque, ya que al cargarse la página, el usuario podría identificar que es falsa y así no digitar las credenciales que intentan robar.

- No reaccionar con miedo ante los correos, dado que en la mayoría de los casos existe una amenaza tal como “si no contesta este correo bloquearemos su cuenta” o ¡Han intentado acceder a tu perfil!, Si el último caso lo recomendable es acceder directamente a la cuenta, validar la información y como se ha citado, cambiar las contraseñas periódicamente.

- Tener en cuenta que ningún servicio debe pedir la contraseña en ningún caso distinto a cuando se va a acceder a la misma.

- En algunos casos los ciberdelincuentes envían correo phishing de bancos citando que eres cliente de ese banco, pero si se valida no se tiene ningún producto o servicio con ese supuesto banco, es otra alerta ya que muchos usuarios ingenuos

pueden ingresar datos pese a que no tienen cuenta, y es allí donde brindan la información a los ciberdelincuentes que posteriormente podrán utilizar.

- Otro caso puede ser la sorpresa de haber ganado algún premio de manera inesperada. Es cierto que el hecho de ganar algo puede alegrarnos, pero ¿Como pude ganar algo en lo que nunca he participado? Este caso se viene presentando desde hace bastante tiempo, por ejemplo el caso de la lotería de Microsoft o la fortuna del rey de Nigeria donde lo único que pueden pedir es el usuario u otros datos básicos, por medio de esa estafa lo que buscan los ciberdelincuentes es recopilar información de las víctimas, las cuentas de correo para de pronto el envío de spam, suplantación de identidad, etc.

- En algunos casos pueden llegar correos solicitando información donde se nota que no tiene mayor información de contacto, son correos muy básicos que no suministran información del remitente, ante estos casos lo mejor es eliminarlos de inmediato.

- Validar que la información sea coherente, es validar si por ejemplo llega un correo de supuestamente una entidad bancaria, pero el cuerpo del correo no tiene nada que ver con los servicios que presta o con los productos que se tienen contratados, al igual que recibir un correo de una supuesta respuesta donde no se tiene conocimiento de la solicitud inicial, en estos casos los correos pueden contener

malware o spam, para este caso se debe evitar dar clic sobre el cuerpo del correo, los links si llega a haber y no abrir o descargar los archivos adjuntos.

- Validar la información de la hora de envío, ya que es otro tip a tener en cuenta, si se valida por ejemplo un correo que sea enviado en la madrugada es posiblemente un correo enviado como spam o desde una botnet.

- Procurar no abrir los archivos adjuntos en la máquina o descargarlos, se sugiere tener un analizador de archivos antes de su descarga y otra manera para evitar abrir un archivo infectado es utilizar un visualizador en línea ya que de esa manera el contenido se abrirá en formato html y se puede validar el contenido evitando que se ejecute el malware que pueda tener.

- Tener visibles las extensiones de los archivos, ya que aunque muchos correos electrónicos cuentan con antivirus que valida la información o los archivos, puede que envíen un archivo adjunto con extensión .exe, si es el caso por ningún motivo lo ejecute, ya que puede ser un malware y al darle clic se le están otorgando los permisos que necesita para poder realizar las acciones que tenga programadas.

- Procurar no instalar plugins en los navegadores si no son necesarios, dado el caso de instalarse validar que sea desde la página del fabricante y que sea la versión más actualizada. En este caso es bueno aclarar que existen herramientas para mitigar el riesgo de ataques.

- Aunque es una medida extrema pero es la mejor, no confíe en ningún correo electrónico, ya que por lo general los ciberdelincuentes que van a realizar este tipo de ataques clonan las páginas y suplantan la identidad bien sea de personas naturales como de personas jurídicas, es por ello que si no se tiene conocimiento del remitente, en lo posible elimínelo, o si desea leer de que trata, evite dar clic sobre el cuerpo del correo, abrir los archivos que llegan adjuntos o ingresar a los links que puedan llegar en el mismo. Para ese caso es mejor que primero se valide si es un correo legítimo, si es así y debe acceder a un hipervínculo procure digitarlo directamente en el navegador ya que puede haber alguna acción interna o en segundo plano que no es percibidle para el usuario final, pero en ese momento puede estar realizándose el ataque.

Vale aclarar que los sistemas Windows son los que se encuentran más expuestos dado que son los más populares y usados a nivel mundial, es por eso que las recomendaciones en su mayoría están enfocadas a ese tipo de sistemas, pero a nivel general las recomendaciones son para todos los sistemas, esto quiere decir que se deben implementar medidas de seguridad, mantener actualizado el software, instalar software de sitios oficiales, cambiar las contraseñas que están por defecto.

10.2 RECOMENDACIONES A TENER EN CUENTA PARA FUTURAS INVESTIGACIONES

Para proyectos futuros se deben tener en cuenta como base las recomendaciones anteriormente mencionadas, pero se puede profundizar aún más si se busca realizar a nivel empresarial, puede ser desde pymes hasta grandes multinacionales, donde la línea base siempre debe ser la concientización a las personas en el sentido de la seguridad, que pese al concepto o paradigma de pensar “y a quien le va a interesar mi información, lo que yo tengo no le importa a nadie”, es vital que se salgan de esa idea y sean conscientes que la tecnología nos ayuda a mejorar muchas tareas y procesos, y de la misma manera se tienen que establecer buenas prácticas para el uso de las mismas, de esa manera se pueden mitigar los riesgos a los que se pueden ver expuestos. En la actualidad, la tecnología ha avanzado de una manera inimaginable, dado que hace unos años el uso de los computadores era casi exclusivo, pero hoy en día se pueden encontrar computadores en casi todos los hogares y empresas, pero no solo eso, también se cuenta con tecnología tal como dispositivos móviles como Tablet, Smartphone, etc., el uso de esos dispositivos se ha convertido en algo esencial, tanto así que toda la información se puede encontrar en los mismos, y hasta las transacciones se han pasado en gran porcentaje al medio virtual, también el uso de redes sociales, que por ignorancia se podría decir, las personas no tiene ciertas precauciones y publican toda la información, es por ello que los ciberdelincuentes ven esas redes con un alto potencial de negocio para ellos, y es por eso que atacan por ese medio.

De acuerdo con lo anterior, para el caso de las empresas, se convierte en un riesgo aún más relevante, por eso se deben adoptar mayores medidas para garantizar la continuidad del negocio y es por esa razón que se debe hablar de una política de seguridad de la información, y se deben establecer muchos canales de control y medidas de seguridad; para eso existen varios tipos de estándares o buenas prácticas, las cuales se pueden adoptar para mitigar el riesgo.

Para el caso empresarial se pueden tener en cuenta las siguientes recomendaciones:

- ITIL: Certificado de mejores prácticas, se cambia el paradigma de pensar que las áreas de tecnología informática son los administradores de dispositivos, a que sean administradores de servicios de tecnologías.

- COBIT: Guía de mejores prácticas que se enfoca en control y supervisión de la tecnología de la información. Trabaja un modelo de madurez donde se busca evaluar el control de procesos en 5 escalas donde (0) es que no existe y (5) es optimizado.

- OSSTMM: Metodología abierta que se utiliza para realizar pruebas y así validar el nivel operacional de la seguridad operacional.

- COMMON CRITERIA: Estándar internacional que define criterios de seguridad de los productos o sistemas de la tecnología informática, con este estándar se pueden establecer los requisitos a todos los niveles de seguridad.

- MAGERIT: Metodología para el análisis y gestión de riesgos de los sistemas de información.

- ISM3: Estándar para implementación de un sistema de gestión de la seguridad de la información, el cual se puede implementar por si solo o para mejorar sistemas basados en ITIL, ISO 27001 o Cobit.

- OCTAVE: Es una evaluación de vulnerabilidades y amenazas de los recursos tecnológicos desde el punto de vista de los usuarios hacia la infraestructura tecnológica. Se enfoca en el riesgo organizacional direccionado en la estrategia y la práctica, de esta manera busca identificar la información a nivel gerencial, operacional y de usuario final.

También se debe tener el enfoque de seguridad no solo en los equipos de cómputo de mesa y portátiles, sino también de los dispositivos móviles como la Tablet o los Smartphone, ya que son los más utilizados a nivel mundial, por esa razón son los dispositivos que se deben proteger porque los llevamos en todo momento; dado los servicios que prestan esos dispositivos, si se instalan aplicaciones no oficiales o se instalan roms cocinadas (que han sido modificadas), las mismas pese a que pueden

funcionar de manera más fluida en realidad suelen ser más vulnerables dado que en la gran mayoría lo que hacen es eliminar programas o registros que puede que hagan que los dispositivos no funcionen de manera muy fluida, pero si se desinstalan u omiten registros, estos pueden hacer el sistema más vulnerable y es allí cuando los ciberdelincuentes aprovechan esas posibles vulnerabilidades para atacar.

11. RESULTADOS Y DISCUSIÓN

11.1 DISCUSIÓN

Teniendo en cuenta lo publicado en el proyecto “Botnet” (ARAUZO ALMIRON, 2009)[56], en lo referente al término ciberguerra, es muy válido lo que trata relacionado con las botnet, ya que como se ha visto en el presente documento, los botmasters buscan capturar la mayor cantidad de máquinas posibles para usarlas en su beneficio, en este caso para realizar ataques en la mayoría de los casos de denegación de servicios y con esto sacar de servicio páginas o procesos que se estén ejecutando y ello afecta la funcionalidad de muchos servicios, en el peor de los casos se puede ver como ataques dirigidos, y como se vio el 12 de mayo de 2017 el ataque de rasonmware WannaCry que fue un ataque dirigido a los sistemas operativos de Microsoft Windows, y como en todos los casos de este tipo de ataques, se solicitaba para des encriptar la información el pago en criptomonedas Bitcoin; ese ataque se realizó a nivel mundial y se vieron afectadas grandes compañías como lo son FedEx, Latam y Telefónica. Este ataque se realizó sobre todo porque en las compañías tenían equipos con sistemas operativos que ya no tenían actualizaciones y dado ello no se podían parchar o actualizar los registros mediante los cuales se eliminan las vulnerabilidades que tenían los sistemas

[56] Botnet. (https://upcommons.upc.edu/bitstream/handle/2099.1/8692/Mem%C3%B2ria%20Arauzo%20Almiron,%20Valentin.pdf)

operativos, es en este punto cuando los atacantes tienen conocimiento de exploits o zero days, los cuáles al infectar la máquina hacen que se ejecute un programa el cual aprovecha esas vulnerabilidades para acceder y poder tener éxito en su ataque. Es por esta razón que es importante mantener el software actualizado.

De acuerdo con lo tratado por (RIPOLL CERVERA, 2015)[57], en el estudio realizado, se puede ver que cuando se estudia el tráfico de red de las máquinas se puede detectar cuando se encuentre infectado con algún tipo de malware que convierta la máquina en un bot, el cual utilizarán los ciberdelincuentes para realizar delitos informáticos, al igual que se evidencia cuando los mismos utilizan los recursos de la víctima para su beneficio, en la mayoría de los casos los recursos y las máquinas víctimas son usados para hacer ataque de denegación de servicios dirigido (DDos); como se evidenció a lo largo del presente documento, los ciberdelincuentes utilizan malware para poder acceder a las máquinas de las víctimas usando en muchos de los casos técnicas básicas y que en muchos casos suelen tener éxito dado que son fallos o vulnerabilidades que se detectan en el software y que los usuarios en muchos de los casos no tienen conciencia de la importancia de la información y que los sistemas están expuestos constantemente a ataques por las vulnerabilidades identificadas a los mismos, al igual que no tienen software antimalware o antivirus que ayuden a identificar y mitigar el riesgo al que se encuentran expuestos. Tal como

[57] Detección y bloqueo de botnets mediante la combinación de técnicas basadas en el tráfico de red http://www.issi.uned.es/Master_ISSI/WebMISSI/RepositorioTFM/2015/15S_MemoriaTFdM_ISW_TipoB_Juan_Enrique_Ripoll_Cervera.pdf

lo demostraron, solo se usaron 4 máquinas virtuales y se pudo ver como se comportaba un ataque, eso con un equipo con recursos básicos, es así que se puede ver la complejidad de los ataques, ya que los ciberdelincuentes no necesitarán muchos recursos, ya que tomarán los de las víctimas para realizar sus actividades ilícitas.

11.2 CONCLUSIONES

Al identificar el comportamiento de las botnets, es posible establecer mecanismos mediante los cuales se puede proteger la integridad de los equipos de cómputo y de la información.

Conociendo los riesgos a los que se encuentran expuestos los activos de información, es posible concientizar a los usuarios de la importancia de la información que se tiene almacenada, además de generar conciencia del manejo de la información y el tratamiento de la misma.

Es importante implementar mecanismos de control y seguridad mediantes los cuales se pueden proteger los equipos de cómputo y la información almacenada.

Es necesario adquirir una cultura de la seguridad, dado que con el avance de la tecnología también se incrementan las vulnerabilidades que se pueden presentar,

es por ello que al darle la importancia que se merece la información y los datos, se hace necesaria la implementación de ciertas medidas de seguridad para mitigar ese riesgo.

12. DIVULGACIÓN

El presente documento se divulgará en el repositorio de información de la Universidad Nacional Abierta y a Distancia UNAD.

Bibliografía

ANDRADE GUZMAN, J. M. (2010). *UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO*. Obtenido de http://www.ru.tic.unam.mx:8080/tic/bitstream/handle/123456789/1726/31.pdf?sequence=1&isAllowed=y

AprendeLibre, G. (s.f.). *GCF AprendeLibre*. Obtenido de https://www.gcfaprendelibre.org/tecnologia/curso/virus_informaticos_y_antivirus/los_virus_informaticos/1.do

ARAUZO ALMIRON, V. (2009). Obtenido de https://upcommons.upc.edu/bitstream/handle/2099.1/8692/Mem%C3%B2ria%20Arauzo%20Almiron,%20Valentin.pdf

Avast. (s.f.). *Avast.com*. Obtenido de https://www.avast.com/es-es/c-rootkit

CANO, J. J. (s.f.). Obtenido de http://52.0.140.184/typo43/fileadmin/Revista_119/Editorial.pdf

CCM. (s.f.). Obtenido de http://es.ccm.net/contents/163-sistema-de-prevencion-de-intrusiones-ips

COBB, S. (24 de Enero de 2017). *WE LIVE SECURIRY BY ESET*. Obtenido de http://www.welivesecurity.com/la-es/2014/10/27/botnets-como-combatirlas

COMERCIO, L. C. (Noviembre de 2015). Obtenido de https://www.consumidor.ftc.gov/articulos/s0011-software-malicioso

COMISION DE REGULACION DE LAS COMUNICACIONES. (23 de Diciembre de 2009). Obtenido de http://itcomunicaciones.net/Resolucion%202258.pdf

CONGRESO DE COLOMBIA. (24 de JULIO de 2000). *DIARIO OFICIAL*. Obtenido de https://docs.supersalud.gov.co/PortalWeb/Juridica/Leyes/L0599_00.pdf

CONGRESO DE COLOMBIA. (08 de Julio de 2005). *DIARIO OFICIAL*. Obtenido de http://www.secretariasenado.gov.co/senado/basedoc/ley_0962_2005.htm

CONGRESO DE COLOMBIA. (16 de Julio de 2007). *DIARIO OFICIAL*. Obtenido de http://www.secretariasenado.gov.co/senado/basedoc/ley_1150_2007.html

CONGRESO DE COLOMBIA. (31 de Diciembre de 2008). *DIARIO OFICIAL*. Obtenido de http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html

CONGRESO DE COLOMBIA. (5 de Enero de 2009). *Diario Oficial*. Obtenido de http://acueductopopayan.com.co/wp-content/uploads/2012/08/ley-1273-2009.pdf

CONGRESO DE COLOMBIA. (24 de Junio de 2011). *MINTIC*. Obtenido de http://www.mintic.gov.co/portal/604/articles-3709_documento.pdf

CUBIDES CORRALES, I. D., MURCIA GUZMAN, M. O., & ZAPATA PAREJA, C. A. (2015). Obtenido de http://bibliotecadigital.usb.edu.co/bitstream/10819/4208/1/Tecnicas_Deteccion_Analisis_Zapata_2015.pdf

DIAZ, A. (7 de Noviembre de 2016). Obtenido de http://informaticaseguridaddiazpech.blogspot.com/2016/11/antivirus-preventores.html

Diccionario Actual. (s.f.). Obtenido de https://diccionarioactual.com/p2p/

GARCIA, C. (26 de Agosto de 2010). *hacking-etico.com*. Obtenido de https://hacking-etico.com/2010/08/26/hablemos-de-spoofing/

GARCIA, S. (1 de Junio de 2011). Obtenido de https://www.researchgate.net/profile/Sebastian_Garcia6/publication/237836318_Deteccion_de_botnets_basada_en_algoritmos_geneticos/links/0c96051bc3066460e5000000/Deteccion-de-botnets-basada-en-algoritmos-geneticos.pdf

Homo erectus. (17 de Junio de 2013). *BLOGSPOT.COM*. Obtenido de http://ciberdelitoss.blogspot.com.co/2013/06/definicion.html

HUERTA, A. V. (2 de Octubre de 2000). *SEGU-INFO SEGURIDAD DE LA INFORAMCIÓN*. Obtenido de https://www.segu-info.com.ar/fisica/seguridadfisica.htm

ISOTOOLS.ORG. (s.f.). Obtenido de https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001

LAB, K. (s.f.). *KASPERSKY LAB*. Obtenido de https://latam.kaspersky.com/resource-center/definitions/zero-day-exploit

LABS, A. (31 de Diciembre de 2011). *[A]NTRAX - [L]ABS*. Obtenido de http://www.antrax-labs.org/2011/12/taller-de-malwares-4-botnets.html

LATINOAMERICA, E. (14 de Mayo de 2010). *ESET LATINOAMERICA*. Obtenido de https://www.youtube.com/watch?v=EoATrwF4DdM

LATINOAMERICA, E. (14 de Diciembre de 2010). *ESET LATINOAMERICA*. Obtenido de http://www.eset-la.com/pdf/prensa/informe/tendencias_2011_las_botnet_y_el_malware_dinamico.pdf

mejor-antivirus.es. (s.f.). Obtenido de http://www.mejor-antivirus.es/preguntas/antimalware.html

MIERES, J. (24 de Octubre de 2009). *BLOGSPOT.COM*. Obtenido de http://mipistus.blogspot.com.co/2009/10/zeus-botnet-y-su-poder-de-reclutamiento.html

MINTIC. (1999). Obtenido de http://www.mintic.gov.co/portal/604/w3-article-3679.html

MINTIC. (2009). Obtenido de http://www.mintic.gov.co/portal/604/w3-article-3705.html

OFICINA DE SEGURIDAD DEL INTERNAUTA. (14 de Marzo de 2014). Obtenido de https://www.osi.es/es/actualidad/blog/2014/03/14/que-es-una-botnet-o-una-red-zombi-de-ordenadores

protejete.wordpress.com. (s.f.). Obtenido de https://protejete.wordpress.com/gdr_principal/definicion_si/

QUINTERO, J. (2013). Obtenido de http://virusinformaticosyantivirus.blogspot.com/2013/08/antivirus-identificadores-esta-clase-de.html

REAL ACADEMIA ESPAÑOLA. (2017). *REAL ACADEMIA ESPAÑOLA*. Obtenido de http://dle.rae.es/?id=JxlUKkm

RIPOLL CERVERA, E. (2015). Obtenido de http://www.issi.uned.es/Master_ISSI/WebMISSI/RepositorioTFM/2015/15S_MemoriaTFdM_ISW_TipoB_Juan_Enrique_Ripoll_Cervera.pdf

RIVERO, M. (13 de Enero de 2011). *infospyware.com*. Obtenido de https://www.infospyware.com/articulos/%C2%BFque-son-los-virus-informaticos/

RODRIGUEZ VARELA, J. (2013 de Agosto de 2013). *WE LIVE SECURITY BY ESET*. Obtenido de http://www.welivesecurity.com/la-es/2013/08/01/blackhat-como-crear-una-botnet-de-1-000-000-de-navegadores/

ROUSE, M. (Noviembre de 2012). *searchdatacenter.techtarget.com*. Obtenido de http://searchdatacenter.techtarget.com/es/definicion/Ataque-de-denegacion-de-servicio

SANCHEZ SOLEDAD, J. R., & SANTILLAN ARENAS, J. (2010). *UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO*. Obtenido de http://www.ru.tic.unam.mx:8080/tic/bitstream/handle/123456789/1726/31.pdf?sequence=1&isAllowed=y

SEGU.INFO. (s.f.). *SEGU.INFO SEGURIDAD DE LA INFORMACION*. Obtenido de https://www.segu-info.com.ar/proteccion/deteccion.htm

SERRANO, F. (26 de Noviembre de 2012). *blogspot.com*. Obtenido de http://serranop4030.blogspot.com/2012/11/resumen-de-antivirus.html

SUPERINTENDECIA FINANCIERA DE COLOMBIA. (29 de Noviembre de 2012). *SUPERINTENDECIA FINANCIERA DE COLOMBIA*. Obtenido de https://www.superfinanciera.gov.co/jsp/loader.jsf?lServicio=Publicaciones&lTipo=publicaciones&lFuncion=loadContenidoPublicacion&id=20145

URUEÑA CENTENO, F. J. (16 de Enero de 2015). *ieee.es*. Obtenido de http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO09-2015_AmenazaCiberataques_Fco.Uruena.pdf

RAE – ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA - UNAD

Título	Monografía de estudio sobre el análisis de la afectación de las botnets sobre los equipos de cómputo personales
Autor	Andrei Luciano Jiménez Arias
Año	2018
Palabras Claves	Botnet o red de robots, ciberdelincuentes, denegación de servicios, malware, seguridad de la información, delitos informáticos.
Descripción	El proyecto es una monografía de investigación, la cual se presentará desde un enfoque cualitativo, dado que se realizará desde el análisis de material bibliográfico que busca resolver la pregunta de investigación que se formuló.
Fuentes Bibliográficas	• ARAUZO ALMIRON, V. (2009). Obtenido de https://upcommons.upc.edu/bitstream/handle/2099.1/8692/Mem%C3%B2ria%20Arauzo%20Almiron,%20Valentin.pdf • RIPOLL CERVERA, E. (2015). Obtenido de http://www.issi.uned.es/Master_ISSI/WebMISSI/RepositorioTFM/2015/15S_MemoriaTFdM_ISW_TipoB_Juan_Enrique_Ripoll_Cervera.pdf • GARCIA, S. (1 de Junio de 2011). Obtenido de https://www.researchgate.net/profile/Sebastian_Garcia6/publication/237836318_Deteccion_de_botnets_basada_en_algoritmos_geneticos/links/0c96051bc3066460e5000000/Deteccion-de-botnets-basada-en-algoritmos-geneticos.pdf • SANCHEZ SOLEDAD, J. R., & SANTILLAN ARENAS, J. (2010). UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO. Obtenido de http://www.ru.tic.unam.mx:8080/tic/bitstream/handle/123456789/1726/31.pdf?sequence=1&isAllowed=y • CUBIDES CORRALES, I. D., MURCIA GUZMAN, M. O., & ZAPATA PAREJA, C. A. (2015). Obtenido de http://bibliotecadigital.usb.edu.co/bitstream/10819/4208/1/Tecnicas_Deteccion_Analisis_Zapata_2015.pdf
Contenido	**Resumen** En el presente documento se encontrará la información relacionada con el tema de los botnets, que son, para que se usan, como pueden llegar a afectar a los equipos de cómputo, con que finalidad se utilizan, quienes las manejan y algunos tips que se deben tener en cuenta para evitar el ataque de los mismos. De la misma manera se podrán identificar los tipos de ataques que se pueden presentar por parte de los ciberdelincuentes para buscar el acceso a los equipos de cómputo para de esta manera realizar actividades ilícitas para el beneficio de los mismos. Al conocer cómo se comportan los botnets, con que finalidad son utilizados, que consecuencia puede traer la instalación de uno de esos robots en los equipos de cómputo, se busca la concientización de los usuarios finales para que adopten buenas prácticas para la salvaguarda de la información y la protección de los equipos de cómputo y la información almacenada en los mismos. **Formulación del problema**

	¿El análisis de la afectación de las Botnets y su comportamiento ayudará a crear conciencia a los usuarios finales para evitar implementar medidas de seguridad y controles para que sus equipos de cómputo no se vean afectados y expuestos a delitos informáticos y a una posible pérdida de información? **Objetivo general** Identificar los ataques informáticos a los que se encuentran expuestos en la actualidad los usuarios finales y el riesgo que corren al ser infectados por algún malware que los haga parte de una botnet y los tipos de delitos informáticos más comunes que se presentan y en los que se podrían ver involucrados si son parte de una Botnet. **Objetivos específicos** • Identificar los ataques informáticos más conocidos en la actualidad. • Citar los tipos de malware más conocidos y utilizados por los ciberdelincuentes en la actualidad. • Listar los delitos informáticos más relevantes de los últimos tiempos. • Entender cómo se compromete la integridad de un equipo que se encuentre en una botnet y su comportamiento. • Crear una guía para el usuario final donde encontrará recomendaciones para que se deben tener en cuenta con el fin de mitigar el riesgo y evitar ser parte de una Botnet o de ser parte de un delito informático.
Metodología	Se establece que el tipo de metodología que se maneja en este proyecto es investigativa, la cuál puede ser aplicada a todos los campos, dado que se toman casos reales a lo largo de la historia donde se evidencian las causas y consecuencias presentadas para de esa manera aplicar el conocimiento para dar solución de problemas.
Conclusiones	Al identificar el comportamiento de las botnets, es posible establecer mecanismos mediante los cuales se puede proteger la integridad de los equipos de cómputo y de la información. Conociendo los riesgos a los que se encuentran expuestos los activos de información, es posible concientizar a los usuarios de la importancia de la información que se tiene almacenada, además de generar conciencia del manejo de la información y el tratamiento de la misma. Es importante implementar mecanismos de control y seguridad mediantes los cuales se pueden proteger los equipos de cómputo y la información almacenada. Es necesario adquirir una cultura de la seguridad, dado que con el avance de la tecnología también se incrementan las vulnerabilidades que se pueden presentar, es por ello que al darle la importancia que se merece la información y los datos, se hace necesaria la implementación de ciertas medidas de seguridad para mitigar ese riesgo.
Recomendaciones	Se debe tener en cuenta que las aplicaciones están creadas para lo que fueron hechas, esto quiere decir que las medidas que se deben implementar

	son diversas, no se puede dejar la seguridad de la información solo en una medida de seguridad, para ser más claro, para estar protegidos de los ciberataques no es posible solo con un software, se debe partir desde la conciencia del usuario, que sepa a lo que se encuentra expuesto en la actualidad, que tengan conciencia del valor de la información y de los dispositivos que maneja, llámense portátiles, equipos de escritorio, smartphones, etc, luego se deben establecer medidas de seguridad que se citaran a continuación: • Instalar antivirus de casas de software reconocidas o de buena reputación como por ejemplo Symantec, Eset, Panda, Avast, AVG, etc., de igual manera se recomienda que se mantenga actualizado y con escaneo en línea, ya que si llegan a detectar alguna vulnerabilidad, publicarán la solución para mitigar el riesgo al que se pueda ver expuesto el usuario final. • Instalar antivirus con capacidad proactiva que permita detectar archivos maliciosos como Eset NOD32, Eset Smart Security con protección contra Botnets, Panda Gold Protección, Avast – antiphishing. • Mantener actualizado el software, ya que así se puede mitigar el riesgo asociado a vulnerabilidades que se puedan encontrar en el mismo. • No ingresar a páginas web de dudosa reputación. • No ingresar a páginas donde pidan credenciales como usuario, contraseña, pin, etc., desde links, mejor ir directamente a la barra de direcciones y digitar la url a la que se desea acceder. • Si es necesario acceder desde un link, siempre validar que la dirección esté bien escrita, dado que si tiene una letra mal o no está completa, se puede estar accediendo a una página clonada en este caso sería un phishing donde al verse como la página original los usuarios digitan la información y es allí donde están entregando todos los datos a los ciberdelincuentes. • Validar que en la página que se está accediendo tiene el protocolo de seguridad (https:// y un candado cerrado) ya que eso garantiza que la información que se está digitando se enviará cifrada, con ello si algún ciberdelincuente realiza un ataque de hombre en medio no podrá ver la información enviada. • Mantener los navegadores actualizados y no instalar plugins sobre el mismo que no se necesiten, dado que por ese medio también pueden los ciberdelincuentes acceder a la información registrada. • Tener una solución de seguridad con firewall para poder tener controlar las comunicaciones del equipo con internet • Descargar software desde los repositorios oficiales, analizar previamente el software antes de la instalación y validando que sea la versión más reciente ya que tendrá resueltas las vulnerabilidades encontradas y corregidos los errores de código que se hubieran detectado. • Utilizar un sistema operativo con soporte, esto quiere decir que se puedan realizar actualizaciones para corregir las vulnerabilidades encontradas para evitar los zero days o exploits.

	• Generar contraseñas robustas, por ejemplo que tengan más de 8 caracteres, que tenga mayúsculas, minúsculas, números y caracteres especiales, esto dificulta que si están mirando lo que se está digitando, sea más complejo el identificarla. • Evitar contraseñas fáciles de identificar tales como nombres de hijos, padres, etc, la mascota o cosas así, ya que uno de los ataques que realizan los delincuentes es la ingeniería social y por ese medio pueden tener fácilmente esos datos, al igual que no dejar de manera pública la información personal, dado que así también pueden realizar análisis y poder tener varias opciones para intentar identificar la posible contraseña, esto teniendo en cuenta que otro ataque que pueden realizar es el de fuerza bruta, esto quiere decir que los delincuentes con la información recopilada pueden hacer un listado de posibles contraseñas y realizar el ataque con la información recopilada hasta poder identificar la contraseña. • No dejar generar contraseñas fáciles de identificar como por ejemplo teclas seguidas o solo numéricas, aunque no es la solución de fondo, por lo menos si es más complicado para el atacante identificar la contraseña, es recomendable implementar un segundo factor de autenticación para así tener mayor seguridad como lo es la aplicación latch, la cual permite bloquear las cuentas que se tengan configuradas para que no se pueda acceder a las mismas sino hasta cuando se active el pestillo. • No utilizar el usuario administrador para el uso de los equipos de cómputo solo para lo necesario, en lo posible generar un usuario que no tenga los permisos de administración ya que si se es atacado, no tendrá los privilegios para poder hacer modificaciones. • Cuando se reciban mensajes por correo electrónico, evitar los que sean de remitentes no conocidos, en caso de abrirse el correo, si tiene archivos adjuntos o enlaces a otros sitios, evitar ejecutar los archivos al igual que validar las extensiones de los mismos y no acceder a los links ya que si se ejecuta el archivo puede tener algún malware o en el caso del link puede que filtre de igual manera software malicioso, en el caso de los hipervínculos en la mayoría de los casos los usuarios esperan que se abra otra ventana direccionando a un sitio, pero puede ser un ataque que solo necesita que se dé clic sobre el link y ya, de esa manera ya se puede estar infectado. • Realizar copias de seguridad periódicamente, dado que si se llega a caer en algún ataque como un rasomware lo recomendable es no pagar lo que piden para recuperar la información. • Realizar periódicamente escaneo de vulnerabilidades en los equipos de cómputo con el software instalado. • No ejecutar programas que piden quitar permisos como el del firewall, antivirus, etc.