risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 02/06/2022
Aceitação/Acceptance: 16/08/2022

Ataques informáticos más comunes en el mundo digitalizado

Javier Guaña-Moya[1], Andrea Sánchez-Zumba[2], Paúl Chérrez-Vintimilla[3], Lorena Chulde-Obando[4], Paulina Jaramillo-Flores[5], Cristian Pillajo-Rea[6].

eguana953@puce.edu.ec; ap.sanchez@uta.edu.ec; pfcherrezv@ucacue.edu.ec; lchulde@yavirac.edu.ec; pjaramillo@itsjapon.edu.ec; cppillajo@pucesa.edu.ec

[1,6] Pontificia Universidad Católica del Ecuador, 170525, Quito-Ambato, Ecuador.

[2] Universidad Técnica de Ambato, 180102, Ambato, Ecuador.

[3] Universidad Católica de Cuenca, 030102, Azogues, Ecuador.

[4] Instituto Superior Tecnológico de Turismo y Patrimonio Yavirac, 170405, Quito, Ecuador.

[5] Instituto Superior Tecnológico Japón, 170525, Quito, Ecuador.

Pages: 87-100

Resumen: El principal objetivo de los ataques informáticos es dañar financieramente a los individuos y las organizaciones de toda índole. Estos ataques se originan por una múltiple variedad de programas, conocidos de manera general como malware. Consecuencia de esta situación las organizaciones aplican diferentes estrategias para prevenir las pérdidas causadas por estos ataques informáticos, valiéndose de los conocimientos de seguridad cibernética que sigue información en tiempo real sobre los últimos datos acerca de la seguridad de la información en los sistemas informáticos. El objetivo de la presente revisión bibliográfica es determinar los tipos más comunes de ciberataques en el mundo actual digitalizado con el fin entender cómo se desarrollan estos y en qué consisten dichas amenazas, conocimiento que permitirá establecer técnicas y métodos para minimizar los efectos que causan sobre la seguridad de la información, considerando que la principal vulnerabilidad dentro de los procesos digitales es el factor humano.

Palabras-clave: Malware; ciberataques; tecnologías de la información (TI); procesos digitales.

Most common computer attacks in the digitized world

Abstract: The main objective of computer attacks is to financially harm individuals and organizations of all kinds. These attacks originate from a wide variety of programs, generally known as malware. As a consequence of this situation, organizations apply different strategies to prevent losses caused by these computer attacks, using cybersecurity knowledge that follows real-time information on the latest data about information security in computer systems. The objective of this bibliographic review is to determine the most common types of cyberattacks in today's digitalized world in order to understand how these are developed and what

these threats consist of, knowledge that will allow establishing techniques and methods to minimize the effects they cause on the information security, considering that the main vulnerability within digital processes is the human factor.

Keywords: Malware; cyberattacks; information technology (IT); digital processes.

1. Introducción

En la actualidad, la mayor parte de las actividades e interacciones económicas, comerciales, culturales, sociales y gubernamentales de los países, en todos los niveles, incluidos los individuos, organizaciones gubernamentales y no gubernamentales, se llevan a cabo en el ciberespacio, por lo que muchas de estas empresas en todo el mundo se enfrentan al problema de los ataques cibernéticos y al peligro de las tecnologías de comunicación inalámbrica, lo cual se ha convertido en un problema desafiante que ha propiciado el continuo y detallado análisis acerca de cómo proteger datos vitales de los múltiples tipos de ataques cibernéticos (Li & Liu, 2021).

El propósito fundamental de los ataques cibernéticos es dañar financieramente a las empresas además de otros fines, tales como militares o políticos. Algunos de estos daños son originados por adware, denegación de servicio distribuido (DDoS), doxing, gusanos, phishing, ransomware, spyware, troyanos y virus, entre otros vectores de ataque. Para ello, diversas organizaciones utilizan diversas soluciones para prevenir los daños causados por los ciberataques, haciendo uso de la seguridad cibernética que sigue información en tiempo real sobre los últimos datos de la tecnología de la información (TI).

El objetivo de la presente revisión bibliográfica es revisar los tipos más comunes de ataques informáticos en el mundo actual digitalizado con el fin entender cómo se desarrollan estos ataques y en qué consisten dichas amenazas, conocimiento que permitirá establecer técnicas y métodos para minimizar los efectos que causan sobre la seguridad de la información, considerando que la principal vulnerabilidad dentro de los procesos digitales es el factor humano.

2. Metodología

Se aplicó la normativa de revisión sistemática de literatura establecida por Kitchenham (2004) para el desarrollo de la presente revisión bibliográfica, lo cual permitió recopilar información relacionada con las preguntas de investigación que se plantearon para la elaboración de la misma. Por tanto, se cumplieron las siguientes fases durante la revisión:

- Planificación de la revisión
- Realización de la revisión
- Análisis de resultados.

2.1. Planificación de la revisión

El objetivo del presente estudio es revisar los tipos más comunes de ataques informáticos existentes en el mundo actual digitalizado, iniciando con la definición de ataques informativos o ciberataques.

Por tanto, para el desarrollo del documento se establecieron las siguientes preguntas de investigación:

P1: ¿Qué es un ciberataque?

P2: ¿Cuáles son los atributos de los ciberataques?

P3: ¿Cuáles son los ataques informáticos más comunes?

Se emplearon bases de datos digitales, tal como ACM Digital Library, IEEE eXplorer, Science Direct Elsevier, Scopus y Springer Link, con documentos que trataban sobre temas asociados a la ciberseguridad, la tecnología y modos de ataques informáticos en la actualidad, identificando entre las fuentes de información revistas académicas y publicaciones técnicas, comprendidas entre los años 2015 y 2022.

La estrategia de búsqueda se basó en aspectos relacionados con las preguntas de investigación, empleando como parámetro las siguientes palabras claves: “malware”, “ciberataques”, “tecnologías de la información” y “procesos digitales”, tanto en idioma español como en inglés.

Además, con el fin de refinar la selección se aplicaron los siguientes criterios (ver Tabla 1).

Criterios de inclusión	Criterios de exclusión
Artículos que definen o explican el término de ciberataque.	Información publicada en sitios web generales.
Documentos que describen las formas y tipos de ciberataques.	Documentos con aportes irrelevantes.
Artículos con información acerca de métodos de seguridad actuales contra los ataques informáticos.	Información de blogs.

Tabla 1 – Criterios de selección

2.2. Realización de la revisión

En esta fase se seleccionaron los artículos en base a las cadenas de búsqueda y criterios de selección, revisando en cada uno los títulos, contenido y conclusiones, actividad que permitió determinar el aporte a las preguntas planteadas.

Como resultado de la búsqueda se identificaron 62 documentos, de los cuales se seleccionaron 33 que cumplieron con los criterios establecidos.

2.3. Análisis de resultados

El concepto de ataques informáticos se determinó al responder la P1: ¿Qué es un ciberataque?

El ataque informático o ciberataque se refiere a aquellas acciones deliberadas contra datos, software o hardware en sistemas o redes informáticas, acciones que pueden destruir, interrumpir, degradar o denegar el acceso. Ante el riesgo permanente de estos ataques, por un lado, gobiernos y organizaciones empresariales de todo el mundo están realizando grandes esfuerzos para proteger sus datos, mientras que por otra parte,

fuerzas armadas y agencias de inteligencia de muchas naciones se preparan de manera constante y activa para participar en ataques cibernéticos, conjuntamente con ataques o contraataques convencionales(Denning & Denning, 2010).

Para detectar o manejar un ataque cibernético, es importante conocer las debilidades de la red, asi como también es necesario que el equipo de seguridad cibernética comprenda el motivo del atacante, a qué datos podrían apuntar y por qué ocurrió el ataque. En consecuencia, es necesaria una planificación adecuada para hacer frente a un ataque cibernético, mediante lo que algunos autores identifican como modelado y análisis de ataques, que permite describir cómo se pueden modelar las amenazas para mitigar los ataques cibernéticos en cualquier organización. Las técnicas de modelado de ataques son importantes para comprender, explorar y validar las amenazas de seguridad en el mundo cibernético(Al-Mohannadi et al., 2016).

P2: ¿Cuáles son los atributos de los ciberataques?

De acuerdo a lo expresado por Kadivar (2014), cada vez que se define ciberataque se hace referencia a cinco atributos claramente identificados, como lo son:

Actores: Mínimo existen dos actores involucrados en cada ciberataque: el propietario del activo al que se dirige y un adversario, lo cual indica que las definiciones de ciberataque no tienen que ver con la naturaleza de los adversarios, debido que las operaciones, tanto ofensivas como defensivas, pueden ser realizadas por naciones, empresas, grupos, colectivos o individuos.

Activos objetivo: Estos activos incluyen: redes y sistemas informáticos, información, programas o funciones residentes o en tránsito en sistemas o redes, infraestructura física operada por computadora y objetos físicos extrínsecos a una computadora, sistema informático o red.

Motivación: Las motivaciones de los ataques cibernéticos incluyen el acceso a información segura o no autorizada, el espionaje y el robo de datos y dinero, seguridad nacional y causas políticas, asi como propaganda o engaño.

Efecto en los activos objetivo: Los ataques cibernéticos resultan en la alteración, eliminación, corrupción, engaño, degradación, inhabilitación, interrupción o destrucción de los activos, tambien en impedir el acceso a los activos. Por tanto, la definición de ciberataques identifican los efectos lógicos, físicos y cognitivos en los activos. La denegación de acceso a los activos es un ejemplo de efectos lógicos, donde los efectos cognitivos incluyen el engaño, es decir, el uso de información falsa para convencer a un adversario de que algo es cierto, mientras que la destrucción de bienes de capital es un caso de efectos físicos.

Duración: Incluye la posibilidad de que un ciberataque se ejecute durante un período prolongado de tiempo.

Respondiendo a la P3: ¿Cuáles son los ataques informáticos más comunes?, se pueden mencionar los siguientes:

2.4. Malware

Malware es el nombre común para muchas versiones maliciosas de un programa, suele ser un código informático destinado a destruir datos o procesos, así como adquirir accesos no autorizados a una red, generalmente se proporciona como un enlace o archivo por correo electrónico para que el usuario haga clic en este o abra el archivo de malware. En una variedad de casos, el ransomware proporciona la carga útil, sin embargo, los ciberatacantes son cada vez más avanzados en las tácticas de solicitar un rescate o robar datos personales confidenciales (Krishnamurthi et al., 2022).

En consecuencia, el malware es un término general que cubre cualquier código que pueda tener un impacto malicioso e indeseable, considerando que todos los intercambios de información conllevan el riesgo de que se intercambie malware. El riesgo puede ser minimizado con el desarrollo e implementación de políticas antimalware apropiadas como parte de un enfoque general de defensa en profundidad. Por ejemplo, el software antivirus ahora es común y debe utilizarse según corresponda, sin embargo, se debe tener cuidado para garantizar que sea adecuado para el propósito previsto y para la plataforma en la que se instalará, para lo cual debe revisarse periódicamente y actualizarse según sea necesario (Smith & Simpson, 2020).

El informe del Grupo de Investigaciones de Seguridad de Cisco, publicado en el año 2016, señala que las redes sociales y los blogs representan áreas altamente sensibles de sufrir ataques cibernéticos, como consecuencia del fácil acceso, la característica de gratuito y la alta popularidad entre los usuarios, aspectos que facilitan el hurto de información sin ser fácilmente detectados, así se tiene el caso de plataformas como WordPress, donde los ataques de suplantación de identidad o el fraude financiero son muy comunes, detectándose una multiplicidad de sistemas empleados que propician todo tipo de software malicioso (Cisco, 2016).

2.5. Virus

En el inicio la referencia de virus informáticos se relacionaba con páginas de juegos en línea, de apuestas o de material pornográfico, no obstante, ha sido demostrado ampliamente que las amenazas no provienen exclusivamente de este tipo de páginas, también son detectadas en sitios de alto tráfico por la frecuencia de visitas por parte de los internautas, tal como webs de compras online, motores de búsqueda e inclusive blogs y redes sociales (Rodríguez-Hidalgo, 2017).

Los virus informáticos son programas especialmente diseñados para ser plagas, debido que proliferan de forma descontrolada y causan graves daños a los datos electrónicos. Estos programas malignos, que se amplifican entre archivos y computadoras, son sorprendentemente similares en virulencia, modos de propagación y vías evolutivas a lo largo del tiempo a los microbios que causan enfermedades infecciosas, principalmente porque ambos virus se transmiten de un huésped a otro y aunque los virus informáticos son una invención humana el desarrollo sigue una ruta biológica bien conocida. Los ancestros relativamente inofensivos evolucionan gradualmente hasta convertirse en

patógenos, desarrollando el huésped mecanismos de defensa adaptativos, que a la vez seleccionan nuevas variantes de virus, alcanzando, finalmente, el equilibrio entre la infección y las defensas del huésped (Wassenaar & Blaser, 2002).

Una encuesta publicada por la empresa ESET (2017), dedicada al negocio de la seguridad en Internet, indica que el 64% de las afectaciones por virus informáticos son causados principalmente por el poco conocimiento de los usuarios. Por otra parte, también señala que el 52,4% de los usuarios no son capaces de detectar el tipo de archivos que descargan del email, mientas que el 22,2% no realiza ningún tipo de análisis a los dispositivos USB que conecta al ordenador, lo cual indica que el riesgo es permanente e inminente.

2.6. Gusanos informáticos

De acuerdo a Ellis (2003) se define como gusano informático al proceso que puede hacer que una copia, posiblemente evolucionada, del mismo se ejecute en una máquina de computación remota, propagándose a sí mismos a través de las redes informáticas al explotar fallas de seguridad o políticas en los servicios de red ampliamente utilizados. Los virus informáticos, al contrario de los gusanos informáticos, no requieren la intervención del usuario para propagarse ni se aprovechan de los archivos existentes, siendo muy rápida la propagación y con capacidad de infectar hasta 359 mil computadoras en menos de 14 horas o menos (Ochieng et al., 2019).

No existen muchos estudios específicos acerca de los gusanos informáticos, situación que no es tan sorprendente considerando que un porcentaje muy pequeño de gusanos realmente afecta la vida diaria, como ralentizar los equipos de computación o reducir el ancho de banda disponible. Aproximadamente el 2 % de todas las cepas de malware que realmente afectan al usuario final son gusanos y el 57 % son virus, lo cual explica por qué cuando la mayoría de las personas se refieren al malware, usan el término virus, debido que es un problema más común para nosotros en comparación con los otros tipos de malware. Sin embargo, si uno de esos gusanos es malicioso, podría hacer que una empresa pierda hasta el 70 % de la productividad y, como consecuencia, el 40 % de los datos de la empresa (Obimbo et al., 2018).

Dentro de la categoría de virus clasificados como gusanos existen varias distinciones, encontrando aproximadamente cinco tipos de gusanos definidos, todos los cuales se clasifican en función de la forma cómo se propagan. Por definición, los gusanos se distribuyen en una red y se ejecutan de forma independiente con la prioridad de multiplicarse y liberar la carga útil (Gharibi, 2011). Los cinco tipos de gusanos se definen de la siguiente manera:

- Gusanos de red: Usan la Internet o la red local para propagarse a través de TCP.
- Gusanos de correo electrónico: Se propagan a través de correos electrónicos y los archivos adjuntos.
- Gusanos IRC: La propagación se produce por canales de retransmisión de Internet**.**
- Gusanos P2P: Propagación por medio de redes peer to peer.
- IM Worms: Propagación a través de aplicaciones de mensajería instantánea.

Asimismo, señala Garibi (2011) que, independientemente del tipo de gusano, existen cinco etapas en el ciclo de vida de un gusano informático a saber: Penetración en la

computadora, activación, búsqueda de víctimas, preparación duplicada, y distribución duplicada.

2.7. Troyanos

Se emplea el término de troyano en informática con la finalidad de describir, la que actualmente es la categoría de malware más común. Troyano es un software malicioso que suplanta procesos legítimos o inofensivos con el fin de acceder a la computadora o móvil de la víctima y desarrollar diversos tipos de acciones maliciosas. Se encuentran ocultos bajo muchas formas, generalmente como archivos de audio, (MP3 o WAV), archivos comprimidos (RAR o ZIP), extensiones del navegador, archivos de actualización, instaladores de software legítimo o app para el celular, entre otras (Muñoz, 2021).

Los troyanos usualmente son utilizados por los atacantes para múltiples objetivos maliciosos, como puede ser el acceder a puertas traseras, conocido como backdoors, controlar el dispositivo de la víctima, extraer información y datos del equipo afectado con el fin de enviarlos al atacante, descargar y ejecutar en la PC o dispositivo del usuario software malicioso adicional, etc. El éxito de estos ataques se fundamenta en la simulación, creando la necesidad al usuario de ejecutar el archivo, caracterizados por el empleo elevado de técnicas de ingeniería social (Muñoz, 2021).

2.8.Spyware

Se conoce como spyware al tipo de software que se instala de forma subrepticia en la computadora de un usuario, monitorea la actividad del mismo e informa a un tercero sobre el comportamiento detectado. De acuerdo a la Comisión Federal de Comercio, que probablemente tiene la autoridad reguladora más poderosa para controlar el software espía, lo define como software que ayuda a recolectar datos e información sobre un individuo u organización sin su conocimiento para luego ser enviada esta información a otra entidad sin el consentimiento del usuario (Urbach & Kibel, 2004). Por tanto, representa un tipo de malware que, esencialmente, es un software que ejerce control sobre la computadora de un usuario sin su consentimiento (Stafford & Urbaczewski, 2004).

Actualmente, el spyware representa una de las amenazas más comunes en Internet para las empresas y los usuarios de manera individual, debido que puede acceder a información confidencial y causar daños en la red. Es un tipo de malware que recopila y transmite información personal a empresas de datos, anunciantes o usuarios externos sin el conocimiento y consentimiento de los propietarios de los datos (Lysenko et al., 2020). Se conocen cuatro tipos principales de spyware que son: Adware, troyanos, cookies de seguimiento, y monitores de sistema.

Cualquiera de las modalidades descritas utiliza funciones de seguimiento para enviar diversa información privada, como una lista de sitios web visitados, direcciones de correo electrónico de contacto del usuario o pulsaciones de teclas en un teclado, capturas de pantalla, actividades en línea en computadoras o dispositivos móviles. Mientras tanto, los datos obtenidos por el software espía pueden contener códigos PIN, códigos de seguridad, números de tarjetas de crédito, etc. Además, el software espía puede activar

cámaras y micrófonos para ver y escuchar a los usuarios sin ser detectados (Drozd et al., 2019).

También algunos tipos de spyware usan análisis no autorizados del estado de los sistemas de seguridad, escanear puertos y vulnerabilidades, mientras que otros pueden instalar otro malware adicional, eliminar ciertos programas y modificar los parámetros de los sistemas operativos. Además, este tipo de malware puede redirigir la actividad del navegador, lo que implica visitar sitios web a ciegas con el riesgo de infección por virus (Lysenko et al., 2020).

2.9. Adware

Corresponde el adware a un tipo de software publicitario que se reproduce y descarga sin consentimiento del usuario, algunas veces, redirige el navegador a páginas web de anuncios. Generalmente la publicidad que se muestra está seleccionada de acuerdo a las posibles preferencias del usuario, las cuales han sido recopiladas previamente en internet o simplemente al realizar búsquedas en cualquier navegador (Gamez, 2017).

El adware se obtiene por medio de software gratuitos al aceptar las condiciones de uso, por lo general no causa daños al sistema y en ciertas ocasiones emplea información de spyware con el fin de catalogar la información de interés del usuario. Generalmente es detectado cuando se evidencia el alto consumo de recursos y por dificultar el empleo de determinadas funciones. Básicamente son causantes de molestias al usuario y limitan de manera sustancial el rendimiento de los sistemas (Rivera, 2013).

Este tipo de malware busca rastrear datos acerca de tu historial de navegación en internet con el propósito de mostrarte anuncios y ventanas emergentes. Es un software no deseado que tiene por finalidad mostrar anuncios personalizados. El adware puede estar diseñado para analizar la ubicación del usuario y páginas web que visitas, mostrando anuncios más enfocados a sus intereses. Generalmente, se instala sin que el usuario se dé cuenta haciéndose pasar por otro tipo de programas (Sánchez-Bautista & Ramírez-Chávez, 2022).

2.10. Ransomware

Corresponde el ransomware a un modelo de malware cuyo objetivo es el de cifrar información y datos valiosos de las organizaciones con el fin de exigir un pago como condición para permitir el acceso a los mismos. Además, también es usado con frecuencia para hurtar información delicada de las organizaciones, exigiendo un pago considerable para no hacer pública la misma a la competencia, autoridades o comunidad en general. Este tipo de ataques están dirigidos principalmente a los datos o la infraestructura crítica de las organizaciones, entorpeciendo o deteniendo operaciones, lo cual representan un dilema para la alta gerencia, por una parte, cancelar el monto del rescate y esperar que los atacantes cumplan con la promesa en cuanto a permitir de nuevo el acceso sin hacer públicos los datos y, por otra parte, no cumplir con el pago del rescate e intentar aplicar procedimientos con el fin de restablecer las operaciones (Barker et al., 2022).

La metodología que aplica el ransomware con el fin de acceder a los sistemas informáticos de las organizaciones son muy parecidos a los ataques cibernéticos de forma más amplia, con la diferencia que estos están dirigidos a exigir el pago del rescate. Las metodologías

empleadas para difundir el ransomware permanecen en un cambio continuo a medida que los atacantes encuentren permanentemente formas novedosas de presionar a sus víctimas (Beaman et al., 2021).

El ransomware se diferencia de otros ataques a la ciberseguridad en que el acceso a la información, tal como datos de tarjetas de crédito, propiedad intelectual o información de identificación personal es obtenida de manera furtiva y posteriormente es exfiltrada con fines de monetización; sin embargo, el ransomware representa una amenaza con consecuencias inmediatas sobre las operaciones empresariales. Durante un ataque de ransomware, generalmente las organizaciones poseen muy corto tiempo para evitar, remediar o mitigar el efecto, restablecer los sistemas o establecer comunicación por medio de canales necesarios empresariales, de asociados o de relaciones públicas; por esta razón es primordial que las organizaciones estén preparadas para enfrentarlo, lo cual incluye instruir a los usuarios de los sistemas cibernéticos, establecer equipos de respuesta y tomadores de decisiones empresariales acerca de la importancia de evitar y gestionar riesgos potenciales previo a que sucedan, así como preestablecer las debidas estrategias, procesos y procedimientos para aplicarlos (Barker et al., 2022).

2.11. Phishing

El phishing es un método para intentar obtener detalles potencialmente valiosos, como nombres de usuario, contraseñas o datos médicos, por motivos maliciosos, mediante comunicaciones dirigidas, como correos electrónicos o mensajes, en los que la parte atacante anima a los destinatarios a hacer clic en enlaces a sitios web que ejecutan código malicioso para descargar o instalar malware. Dado que el phishing generalmente requiere que el destinatario realice una acción, se basa en técnicas de ingeniería social y, por lo tanto, muchos contactos parecen provenir de sitios confiables como instituciones financieras o, en el caso de datos de atención médica, administradores de tecnologías de la información (TI) o personal de atención médica (Priestman et al., 2019)the organisation received 858 200 emails: 139 400 (16%(Guaña-Moya, J., et al., 2022).

El enfoque general del phishing se refiere al envío de una gran cantidad de comunicaciones no dirigidas a una amplia gama de destinatarios con la esperanza de que una minoría se convierta en víctima, encontrando diversas variables, tales como:

- Phishing selectivo: Las comunicaciones se dirigen a personas o tipos de personas o empresas específicas.
- Phishing de clonación: Se cambia el contenido de un correo electrónico legítimo para crear un correo electrónico clonado con contenido malicioso.
- Whaling: Las comunicaciones están dirigidas específicamente a objetivos de alto perfil de alto nivel, a menudo supuestamente provenientes de C-suite o departamentos legales (Rashid, 2020).

La intención del phishing es hacer que las víctimas hagan clic e inicien sesión en portales web clonados, como la intranet de la empresa o los sitios bancarios y los sitios de redes sociales como Facebook, Instagram, Twitter o incluso los sitios de Yahoo y Gmail (Grimes, 2020). Una vez que las víctimas desprevenidas hacen clic en la URL enviada por el atacante, en lugar del sitio original es dirigido al sitio falso del atacante. Al intentar iniciar sesión o enviar información en ese sitio web, las víctimas proporcionan al atacante

información confidencial, que incluye identificación de usuario, correo electrónico, contraseña, dirección, número de teléfono móvil, fecha de nacimiento y detalles de la tarjeta de pago, entre otras cosas (Bhardwaj et al., 2020).

Las metodologías aplicadas por los atacantes cibernéticos han mejorado de tal manera que realizan ataques personalizados, generalmente dirigidos a personal de alto nivel y alto valor, como el jefe de recursos humanos, ejecutivos de nivel C como CISO, CTO, CFO o miembros de la junta, constituyendo una forma avanzada de ataque de phishing contra personas, conocida como whaling. Por otra parte, los ataques de spear-phishing son dirigidos a individuos específicos dentro de la organización y son altamente personalizados, tal como miembros del equipo de finanzas, miembros del equipo de seguridad de TI o incluso nuevos empleados (Fruhlinger, 2022).

Además de utilizar portales web clonados, los atacantes también tienen como objetivo la autenticación de dos factores mediante la clonación de contraseñas de un solo uso (OTP) y la creación de códigos QR falsos que, si se escanean con teléfonos móviles, responden ofreciendo grandes descuentos en restaurantes, tiendas de comestibles o servicios doméstico (Bhardwaj et al., 2020).

2.12. Denegación de servicio distribuido (DDoS)

La denegación de servicios distribuidos (DDoS) representa uno de los tipos de ataques más peligrosos que afectan a las computadoras. El objetivo principal de este ataque es derribar la máquina objetivo y hacer que los servicios no estén disponibles para los usuarios legales, lo que se logra, principalmente, dirigiendo muchos equipos para que envíen una gran cantidad de paquetes hacia el computador especifico con el fin de consumir los recursos y hacer que deje de funcionar (Ali et al., 2021).

Señalan Jaafar et al. (2020) que la detección de ataques DDoS es muy desafiante, debido que este es un tipo de ataque cibernético dirigido a una máquina o servidor específico que propicia que estos dejen de brindar servicios a los dispositivos que tiene conectados. Los atacantes en los ataques DDoS pueden formar una red de bots, conocidos como botnet, definidos como una gran cantidad de dispositivos maliciosos que se denominan bots, estando todos estos dispositivos controlados por un atacante principal llamado botnet master, el cual es responsable de elegir y detectar estos dispositivos comprometidos, desarrollando cuatro pasos para formar una botnet (Alarqan et al., 2020). Estos pasos implican: Identificar dispositivos vulnerables, comprometer a los agentes para que actúen como bots, usar un canal C&C entre el atacante y los bots, y apuntar a la víctima usando los bots,

Los atacantes identifican todas las máquinas vulnerables esperadas en la red y las inducen o las dirigen para que reenvíen paquetes o flujos atacados hacia una máquina o servidor específico, usando como métodos para descubrir estas vulnerabilidades herramientas o técnicas como gusanos, puertas traseras o caballos de Troya, pudiendo ser identificados al enviar un correo electrónico que contenga un código malicioso, como un virus (Bhuyan et al., 2015). Esta acción propicia la infección de las máquinas en la red para crear lo que se llama zombis o agentes, los cuales pueden encontrar otros dispositivos vulnerables en la red para expandir la cantidad de equipos de ataque. El atacante principal o el maestro del bot puede comunicarse y administrar estos zombis mediante el uso de protocolos,

obedeciendo las órdenes del atacante a través del servidor de comando y control (Gupta & Badve, 2017).

Todos estos zombis envían paquetes maliciosos hacia el servidor con la incitación del atacante, mientras que el atacante real usa una IP falsificada para ocultar su identidad y ralentizar su descubrimiento. El atacante con sus agentes envía una gran cantidad de paquetes o flujos de baja velocidad hacia la víctima objetivo, lo que conlleva a que el servidor se sobrecargue con paquetes inútiles y evita que los usuarios legítimos obtengan servicios (Ali et al., 2021).

3. Conclusiones

Luego de revisar los tipos más comunes de ataques informáticos se puede deducir que la mejor defensa se fundamenta en el entendimiento de cómo se comportan estos ataques y la manera cómo logran la violación de la seguridad de la información, quedando demostrado que los ciberdelincuentes tienen muchas opciones de perturbar los sistemas, tal como los ataques a través de adware, denegación de servicio distribuido (DDoS), doxing, gusanos, phishing, ransomware, spyware, troyanos y virus, los cuales se basan principalmente en el manejo de la vulnerabilidad humana por medio de la ingeniería social, todo con el objetivo de acceder de forma no autorizado a datos sensibles e infraestructuras críticas.

Por otra parte, las estrategias orientadas a mitigar los diversos tipos de amenazas son variadas, sin embargo, los fundamentos de la seguridad de la información son siempre los mismos, básicamente en el mantenimiento actualizado de los sistemas y las bases de datos de los antivirus, formación de los empleados y usuarios de los sistemas, configuración del cortafuegos para que solamente incluyan en la lista blanca los host y puertos adecuados, mantenimiento de contraseñas seguras, empleo del modelo menos privilegiado del ambiente informático, configurar regularmente copias de seguridad y auditoría constante de los sistemas informáticos con el fin de detectar actividades sospechosas.

Referencias

Alarqan, M. A., Zaaba, Z. F., & Almomani, A. (2020). Detection Mechanisms of DDoS Attack in Cloud Computing Environment: A Survey. En M. Anbar, N. Abdullah, & S. Manickam (Eds.), *Advances in Cyber Security* (pp. 138-152). Springer. https://doi.org/10.1007/978-981-15-2693-0_10

Ali, B. H., Sulaiman, N., Al-Haddad, S. A. R., Atan, R., Hassan, S. L. M., & Alghrairi, M. (2021). Identification of Distributed Denial of Services Anomalies by Using Combination of Entropy and Sequential Probabilities Ratio Test Methods. *Sensors (Basel, Switzerland)*, *21*(19), 6453. https://doi.org/10.3390/s21196453

Al-Mohannadi, H., Mirza, Q., Namanya, A., Awan, I., Cullen, A., & Disso, J. (2016). Cyber-Attack Modeling Analysis Techniques: An Overview. *2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)*, 69-76. https://doi.org/10.1109/W-FiCloud.2016.29

Barker, W. C., Fisher, W., Scarfone, K., & Souppaya, M. (2022). *Ransomware Risk Management: A Cybersecurity Framework Profile (Spanish Translation)*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8374.spa

Beaman, C., Barkworth, A., Akande, T. D., Hakak, S., & Khan, M. K. (2021). Ransomware: Recent advances, analysis, challenges and future research directions. *Computers & Security*, *111*, 102490. https://doi.org/10.1016/j.cose.2021.102490

Bhardwaj, A., Sapra, V., Kumar, A., Kumar, N., & Arthi, S. (2020). Why is phishing still successful? *Computer Fraud & Security*, *2020*(9), 15-19. https://doi.org/10.1016/S1361-3723(20)30098-1

Bhuyan, M. H., Bhattacharyya, D. K., & Kalita, J. K. (2015). An empirical evaluation of information metrics for low-rate and high-rate DDoS attack detection. *Pattern Recognition Letters*, *51*, 1-7. https://doi.org/10.1016/j.patrec.2014.07.019

Cisco. (2016). *Cisco 2016. Informe anual de seguridad* (p. 87). Cisco Systems, Inc. https://www.cisco.com/c/dam/m/es_es/internet-of-everything-ioe/iac/assets/pdfs/security/cisco_2016_asr_011116_es-es.pdf

Denning, P. J., & Denning, D. E. (2010). Discussing cyber attack. *Communications of the ACM*, *53*(9), 29-31. https://doi.org/10.1145/1810891.1810904

Drozd, O., Kharchenko, V., Rucinski, A., Kochanski, T., Garbos, R., & Maevsky, D. (2019). Development of Models in Resilient Computing. *2019 10th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, 1-6. https://doi.org/10.1109/DESSERT.2019.8770035

Ellis, D. (2003). *Worm anatomy and model*. 42-50. https://doi.org/10.1145/948187.948196

ESET. (2017, febrero 11). Las 5 formas más populares de caer en un virus informático. *Semana*. https://www.semana.com/internacional/articulo/formas-mas-comunes-de-infectarse-por-virus-informatico-segun-eset/241863/

Fruhlinger, J. (2022, abril 7). What is spear phishing? Examples, tactics, and techniques. *CSO Online*. https://www.csoonline.com/article/3334617/what-is-spear-phishing-examples-tactics-and-techniques.html

Gamez, J. C. G. (2017). ¿QUÉ HACER CUANDO EL ANTIVIRUS DEJA DE SER UN CONTROL EFECTIVO ANTE UN ATAQUE DE MALWARE? *Universidad Piloto de Colombia*, 8.

Gharibi, D. W. (2011). Studying and Classification of the Most Significant Malicious Software. *Computer Science & Information Systems College*, 5.

Grimes, R. A. (2020, abril 9). 14 real world phishing examples and how to recognize them. *CSO Online*. https://www.csoonline.com/article/3235520/15-real-world-phishing-examples-and-how-to-recognize-them.html

Gupta, B. B., & Badve, O. P. (2017). Taxonomy of DoS and DDoS attacks and desirable defense mechanism in a Cloud computing environment. *Neural Computing and Applications*, *28*(12), 3655-3682. https://doi.org/10.1007/s00521-016-2317-5

Jaafar, A. G., Ismail, S. A., Abdullah, M. S., Kama, N., Azmi, A., & Yusop, O. M. (2020). Recent Analysis of Forged Request Headers Constituted by HTTP DDoS. *Sensors (Basel, Switzerland)*, *20*(14), E3820. https://doi.org/10.3390/s20143820

Kadivar, M. (2014). Cyber-Attack Attributes. *Technology Innovation Management Review*, *4*(11), 22-27.

Kitchenham, B. (2004). Procedures for Performing Systematic Reviews. *Keele, UK, Keele Univ.*, *33*. https://www.researchgate.net/publication/228756057_Procedures_for_Performing_Systematic_Reviews

Krishnamurthi, R., Kumar, A., & Gill, S. S. (2022). *Autonomous and Connected Heavy Vehicle Technology*. Academic Press.

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, *7*, 8176-8186. https://doi.org/10.1016/j.egyr.2021.08.126

Lysenko, S., Bobrovnikova, K., Popov, P., Kharchenko, V., & Medzatyi, D. (2020). Spyware Detection Technique Based on Reinforcement Learning. *CEUR Workshop Proceedings*, *2623*, 11.

Muñoz, F. (2021). Qué es un troyano en informática. *WeLiveSecurity*. https://www.welivesecurity.com/la-es/2021/05/14/que-es-virus-troyano-informatica/

Obimbo, C., Speller, A., Myers, K., Burke, A., & Blatz, M. (2018). Internet Worms and the Weakest Link: Human Error. *2018 International Conference on Computational Science and Computational Intelligence (CSCI)*, 120-123. https://doi.org/10.1109/CSCI46756.2018.00030

Ochieng, N., Mwangi, W., & Ateya, I. (2019). Optimizing Computer Worm Detection Using Ensembles. *Security and Communication Networks*, *2019*, 1-10. https://doi.org/10.1155/2019/4656480

Priestman, W., Anstis, T., Sebire, I. G., Sridharan, S., & Sebire, N. J. (2019). Phishing in healthcare organisations: Threats, mitigation and approaches. *BMJ Health & Care Informatics*, *26*(1), e100031. https://doi.org/10.1136/bmjhci-2019-100031

Rashid, F. Y. (2020, noviembre 24). 8 types of phishing attacks and how to identify them. *CSO Online*. https://www.csoonline.com/article/3234716/8-types-of-phishing-attacks-and-how-to-identify-them.html

Rivera, G. (2013). Malware y algo más. *U@CSIS*, *1*(1), Art. 1. http://investigacionsis.fuac.edu.co/html/RepositorioOJS/ojsfuac/ojs/index.php/UACSIS/article/view/4

Rodríguez-Hidalgo, C. (2017). *Virus informáticos proliferan por desconocimiento de usuarios*. Blog de la Revista Comunicar. https://www.revistacomunicar.com/wp/revista-comunicar/virus-informaticos-proliferan-por-desconocimiento-de-usuarios/

Sánchez-Bautista, G., & Ramírez-Chávez, L. (2022). Amenazas de seguridad a considerar en el desarrollo de software. *XIKUA Boletín Científico de la Escuela Superior de Tlahuelilpan*, *10*(19), Art. 19. https://doi.org/10.29057/xikua.v10i19.8118

Smith, D. J., & Simpson, K. G. L. (2020). *The Safety Critical Systems Handbook: A Straightforward Guide to Functional Safety: IEC 61508 (2010 Edition), IEC 61511 (2015 Edition) and Related Guidance*. Elsevier Science.

Stafford, T. F., & Urbaczewski, A. (2004). Spyware: The Ghost in the Machine. *Communications of the Association for Information Systems*, *14*. https://doi.org/10.17705/1CAIS.01415

Urbach, R., & Kibel, G. (2004). Adware/Spyware: An Update Regarding Pending. *Intellectual Property & Technology Law Journal*, *16*(7), 12-16.

Wassenaar, T. M., & Blaser, M. J. (2002). Contagion on the Internet. *Emerging Infectious Diseases*, *8*(3), 335-336. https://doi.org/10.3201/eid0803.010286

Willard, N. E. (2007). *Cyberbullying and Cyberthreats: Responding to the Challenge of Online Social Aggression, Threats, and Distress*. Research Press.