¿Qué precio tiene la comodidad?
Los riesgos de usar gestores de contraseñas en el ciberespacio

What price convenience? The risks of using password managers in cyberspace

Por Rocio González López y Pedro David Filio Aguilar

Resumen: El artículo examina los riesgos asociados con el uso de gestores de contraseñas en internet, pues estos programas no están exentos de vulnerabilidades. Se presenta una técnica que los ciberdelincuentes utilizan para explotar estas debilidades y acceder a información sensible. Además, se discuten estudios recientes que han revelado fallos de seguridad en navegadores web al permitir la ejecución de códigos maliciosos para extraer contraseñas almacenadas, y se ofrecen recomendaciones prácticas sobre cómo fortalecer la seguridad, como el uso de Autenticación Multifactor.

Palabras clave: contraseñas, ciberseguridad, tecnología, malware, autentificación.

Abstract: The article examines the risks associated with the use of password managers on the Internet, as these programs are not free of vulnerabilities. A technique used by cybercriminals to exploit these weaknesses and gain access to sensitive information is presented. In addition, recent studies that have revealed security flaws in web browsers by allowing the execution of malicious code to extract stored passwords are discussed, and practical recommendations on how to strengthen security, such as the use of Multifactor Authentication, are offered.

Keywords: passwords, cybersecurity, technology, malware, authentication.

El ciberespacio es el entorno virtual en donde conviven las tecnologías de la información y la comunicación, como el internet que, con su crecimiento, ha facilitado la consulta de información a través de los navegadores. Las cuentas de usuarios aparecieron y estos comenzaron a coleccionar contraseñas de múltiples sitios, por lo cual surgió la necesidad de contar con un lugar seguro para resguardarlas debido a la dificultad de recordarlas. Un gestor es un programa o servicio que facilita el almacenamiento seguro de las diversas contraseñas empleadas para acceder a diferentes aplicaciones o sitios web (Paniagua, 2022: 52). Actualmente, los navegadores web tienen la opción de autocompletar y almacenar contraseñas mediante gestores integrados, cuya facilidad de uso y conveniencia han sido fundamentales para que los usuarios los utilicen en su vida cotidiana; sin embargo, a pesar de su practicidad, estos gestores presentan vulnerabilidades que pueden comprometer las contraseñas.

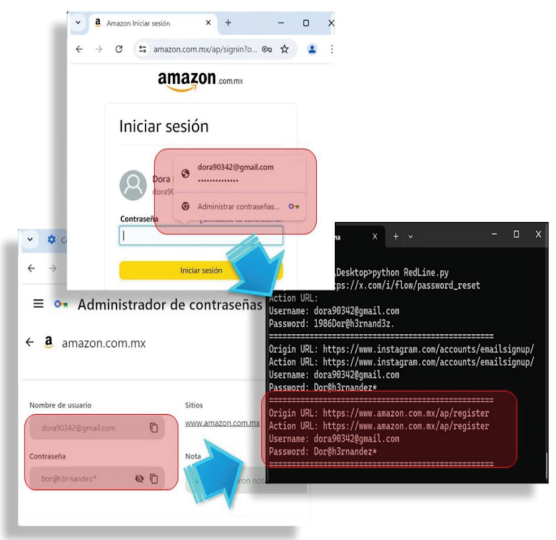
El punto débil más evidente en los gestores de contraseñas integrados es la exposición de los datos a cualquier persona que tenga acceso físico al equipo de cómputo; es sumamente fácil extraer las contraseñas almacenadas en un equipo sin medidas de seguridad. Los gestores cifran la información, no obstante, esta protección es insuficiente para los ciberatacantes que aprovechan cualquier vulnerabilidad de los métodos de protección para ejecutar un código malicioso. Puesto

Montaje digital: Luis Ángel Velázquez

que las credenciales del usuario actúan como la puerta de entrada al entorno corporativo de sus potenciales víctimas, los cibercriminales utilizan numerosas técnicas para obtenerlas (Guerra, 2023). Tal es el caso del *malware* RedLine Stealer de la familia de los troyanos, conocida como *stealer* o *infostealer*, que se dedica a robar información de los usuarios desde los navegadores (CSIRT, 2022).

De acuerdo con Herrero (2023), existen análisis que tienen como objetivo encontrar las debilidades presentes en los sistemas, pero sin llegar a explotarlas. Este tipo de práctica es común en el ámbito de la ciberseguridad para identificar las fallas en las aplicaciones, como los navegadores web, antes de que lo hagan los ciberdelincuentes. En un ejercicio académico reciente se observó que los gestores de contraseñas no protegen del todo los datos, pues permiten que se ejecuten los códigos maliciosos para extraerlas. La prueba consistió en una página web desplegada en el entorno del laboratorio, en la cual se inyectó el código del *malware* RedLine que simuló la extracción de las contraseñas almacenadas en el navegador, que, por cierto, es uno de los más populares (Figura 1); se expuso que una vulnerabilidad no solucionada puede ser explotada por cualquiera, lo cual es crítico, porque se expone información confidencial, como las contraseñas de los usuarios.

Figura 1. Resultado del ejercicio de extracción de contraseñas almacenadas en un navegador de prueba



Fuente: elaboración propia.

A partir de este resultado, se sugiere aplicar medidas de seguridad como la Autenticación Multifactor (MFA) para verificar a un usuario por medio de dos o más formas de identificación con el empleo de 1) algo que sabe (una contraseña), 2) algo que el usuario tiene (teléfono celular o un token) o 3) algo que evitará el acceso no autorizado (reconocimiento facial, huellas dactilares o voz), incluso si las contraseñas son comprometidas. Además, mantener actualizado el antivirus y realizar escaneos regulares ayudará a detectar y eliminar *malware*. Asimismo, se debe educar a los usuarios para que conozcan los riesgos que implica navegar en la web sin las medidas de seguridad correspondientes y reducir la probabilidad de sufrir pérdidas de información. Por último, se recomienda elegir gestores de contraseñas dedicados exclusivamente al resguardo de estas, debido a que su configuración es más compleja y más difícil de hackear. Asimismo, es importante estar alerta para actualizar constantemente las medidas de seguridad y estar preparado ante cualquier eventualidad.

Foto IA: Luis Ángel Velázquez

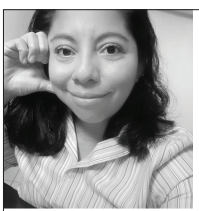
Referencias

CSIRT Equipo de Respuesta ante Incidentes de Seguridad Informática (2022). *Alerta de Seguridad Cibernética | Malware Redline Stealer*. Ministerio del Interior y Seguridad Pública del Gobierno de Chile. <https://csirt.gob.cl/alertas/alerta-de-seguridad-cibernetica-redline/>.

Guerra Soto, Mario (2023). *Ciberinteligencia de la amenaza en entornos corporativos*. España: Ra-Ma S.A. Editorial y Publicaciones.

Herrero Pérez, Luis (2022). *Hacking ético*. España: RA-MA Editorial y Publicaciones.

Paniagua Martín, Fernando y Adolf Rodés Bach (2022). *Marketing digital*. España: Paraninfo.



Rocio González López es Ingeniera en Sistemas Computacionales y discente en la Escuela Militar de Ingeniería en la Maestría en Ciberseguridad y Ciberdefensa.

Pedro David Filio Aguilar es Doctor en Ciencias de la Computación, miembro del Sistema Nacional de Investigadoras e Investigadores (SNII). Se desempeña como docente en la Universidad del Ejército y Fuerza Aérea Mexicanos (UDEFA), en la Escuela Militar de Ingeniería.