Publicado en Madrid el 27/05/2024

Las URLS acortadas pueden contener malware o derivar a la descarga de archivos sin consentimiento

S2 Grupo advierte de que las URL acortadas se han convertido en una herramienta muy utilizada por los ciberdelincuentes para la descarga de malware o archivos sin consentimiento. La compañía también señala que, si bien todos los enlaces cortos no suponen un problema, es necesario seguir algunas recomendaciones para evitar riesgos. Entre otros, aconsejan usar sistemas de análisis de enlaces cortos y no registrar datos personales o contraseñas desde una web a la que se accede desde un link acortado

El equipo de expertos en ciberseguridad y ciberinteligencia de S2 Grupo ha explicado en un comunicado que las URLs acortadas (versión condensada de una dirección web) contienen "una dificultad real en términos de seguridad", ya que es imposible ver la web y el contenido al que se accederá. En este contexto, uno de los principales ciberproblemas es que, mediante la ingeniería social, los ciberdelincuentes pongan enlaces que pueden llevar a las víctimas a webs de descarga de malware, archivos o programas sin consentimiento previo.

Otro de los problemas, es que detrás de algunos enlaces acortados hay empresas que los emplean para la creación de perfiles de usuario, y utilizan técnicas de fingerprinting (huella digital) que permiten rastrear la ubicación a través de la dirección IP y así poder ofrecer anuncios personalizados.

En tercer lugar, desde S2 Grupo se ha incidido en que estos enlaces también pueden llevar a cualquiera a webs fraudulentas que suplantan la identidad de otras para hacer campañas de phising o smishing y, al creer que se está en páginas oficiales de alguna entidad, introducir información confidencial que será útil para los ciberdelincuentes y pondrá en riesgo la privacidad y seguridad.

"Las direcciones web acortadas son muy útiles, sobre todo, en redes sociales. Y, dentro de estas, todavía más en aquellas donde se limita el número de caracteres que podemos utilizar. El problema reside en que en ellas no podemos saber a golpe de vista dónde nos están dirigiendo y esto ha sido aprovechado por los ciberdelincuentes para redirigir a webs que implican la descarga de malware que puede infectar los equipos, entre otros problemas", ha declarado José Rosell, CEO de S2 Grupo.

"Con esto, no estamos diciendo que no se utilicen, a la tecnología no hay que tenerle miedo. Simplemente, hemos de conocer dónde podemos encontrarnos con un ciberpeligro para que podamos actuar de forma responsable y segura para poder disfrutar de ella sin riesgos. En este sentido, la concienciación de todos es esencial", ha continuado José Rosell.

¿Cómo protegerse en el uso de URLs acortadas?

El equipo de ciberinteligencia de S2 Grupo ha señalado que es muy importante tener en cuenta que no todos los enlaces acortados tienen por qué ser peligrosos, pero sí es esencial seguir algunas recomendaciones para utilizarlos de forma cibersegura:

No facilitar ninguna información privada, contraseña o datos de acceso a través de ninguna web a la que hayamos accedido desde de un enlace acortado. Si se necesita hacerlo, es aconsejable volver a introducir la web original a la que se quiere acceder y hacerlo desde ahí.

Verificar que la web a la que se accede es segura y cuenta con el protocolo HTTPS en su inicio y a la izquierda aparece un candado de seguridad.

Si ya se hubiera accedido a la web, es aconsejable realizar un análisis con el antivirus del dispositivo comprometido. Y si se hubieran facilitado contraseñas, es aconsejable cambiarlas.

Utilizar herramientas de Internet, como CheckShortURL o Securi, que permiten analizar los enlaces y conocer su contenido, previsualizar la web a la que se va a acceder y saber si en el link hay algún tipo de malware.

Datos de contacto:
Luis Núñez Canal
S2 Grupo
667574131

Nota de prensa publicada en: Madrid

Categorías: Software Ciberseguridad Dispositivos móviles