# “El Juego del Calamar”: ciberdelincuentes estafan y roban información con estos señuelos

08/11/2021

Algunas personas están aprovechando la popularidad de la serie de **Netflix El Juego del Calamar** (*Squid Game*) para hacer estafas en internet que incluyen **virus troyanos, adware** y ofertas engañosas de disfraces de Halloween.

Y es que el ansia de los fans por tener artículos o ver el afamado drama es tal, que terminan por engancharse a **sitios maliciosos**. En ese sentido, se están lanzando alertas para que no caigan en las trampas.

## Descarga los episodios

Una de las trampas de los **ciberdelincuentes** es engañar a las personas asegurándoles pueden descargar capítulos

gratuitamente. Como un señuelo, quienes no tienen acceso a Netflix son atraídos a esta opción, sin embargo, en lugar de bajar el capítulo bajan malware.

En la mayoría de los casos analizados por *Kaspersky*, se descubrieron **troyanos de descarga capaces de instalar otros programas maliciosos**, aunque también había otros tipos de troyanos y adware. Los ciberdelincuentes pueden obtener dinero y datos sin salir de casa (Foto: Chris Ratcliffe/Bloomberg)

Uno de los esquemas usados por los ciberdelincuentes funcionaba de la siguiente manera: a la víctima se le mostraba una supuesta versión animada del primer juego de la serie, al mismo tiempo, se lanzaba de forma invisible **un troyano que podía robar datos** de los navegadores de los usuarios y enviarlos al servidor de los atacantes. También se creaba un acceso directo desde una de las carpetas, que podía utilizarse para lanzar el troyano cada vez que se iniciaba el sistema.

Sin embargo, esto no fue único para PC, pues también se detectó que hubo técnicas de ciberdelincuentes enfocados a smartphones utilizando la misma estrategia de descarga de los capítulos.

Para ello solicitan **descargar una app** en el dispositivo: ésta pide al servidor de control realizar ciertas tareas para completar la descarga. Entre los comandos está, por ejemplo, abrir una pestaña en el navegador o enviar un SMS a los números recibidos desde el servidor de control. Este troyano se distribuye en tiendas de aplicaciones no oficiales y diversos portales bajo la apariencia de otras aplicaciones, juegos y libros populares. Uno de los ganchos de los ciberdelincuentes fue la venta de disfraces (Foto: Cuartoscuro)

# Compra el traje de El juego del Calamar

Otro de los señuelos que los ciberdelincuentes usaron, aprovechando las fiestas de Halloween, fue lanzar **ofertas de disfraces** temáticos de la serie coreana. De pronto se registró que aparecieron muchas tiendas relacionadas al **Juego del Calamar** y casualmente muchas de ellas ofrecían la vestimenta roja y verde de los actores, con el supuesto de ser "oficiales".

Sin embargo, al comprar en estos sitios, los usuarios se arriesgaron a no recibir la mercancía y a perder su dinero. Además, las potenciales víctimas acabaron compartiendo con los ciberdelincuentes su información bancaria y de identidad personal, ya que se les pide proporcionar detalles de su tarjeta y datos personales, como su dirección de correo electrónico, su dirección de residencia y nombre completo.

# Compite en El Juego del Calamar Online

Con el furor encima, ahora las "clásicas" páginas de phishing, que "transmiten" El Juego del Calamar, también ofrecieron **competir en una versión en línea** del juego para ganar el premio principal: 100 BNB (moneda de una plataforma de intercambio de criptomonedas). No hace falta decir que el jugador nunca recibe la recompensa prometida y acaba perdiendo sus datos o descargando **malware**. No se deben de confiar en sitios extraños y no oficiales (Foto: Youngkyu Park/Netflix/dpa)

# Cómo evitar ser víctima de este

# tipo de estafas

-Verificar la autenticidad de los sitios web antes de introducir datos personales y utilizar sólo las páginas oficiales para ver o descargar películas. Comprobar dos veces los formatos de las URL y la ortografía de los nombres de las empresas.

-Prestar atención a las extensiones de los archivos que se descargan: un archivo de vídeo nunca tendrá una extensión .exe o .msi.

-Utilizar un antivirus que identifique los archivos adjuntos maliciosos y bloquee los sitios de phishing.

-Evitar los enlaces que prometen la visualización anticipada de contenidos y, si tiene dudas sobre la autenticidad de los mismos, comprobarlo con el proveedor de entretenimiento.

Fuente: Infobae