Un grupo de hackers está distribuyendo una forma poderosa de malware troyano a sus víctimas luego de disfrazarlo como un lanzador para uno de los videojuegos más populares del mundo.

El troyano LokiBot surgió por primera vez en 2015 y sigue siendo muy popular entre los delincuentes cibernéticos como un medio para crear una puerta trasera en los sistemas Windows infectados.

Roba información confidencial de las víctimas, incluidos los nombres de usuario, contraseñas, datos bancarios y el contenido de las billeteras de criptomonedas, mediante el uso de un keylogger que monitorea la actividad del navegador y del escritorio.

Ahora, una nueva campaña de LokiBot intenta infectar a los usuarios al hacerse pasar por el lanzador de Epic Games, el desarrollador detrás del popular videojuego multijugador en línea, Fortnite.

Esta campaña de LokiBot recientemente descubierta ha sido detallada por investigadores de seguridad cibernética en Trend Micro, quienes afirman que utiliza una rutina de instalación inusual para ayudar a evitar la detección por parte del software antivirus.

Los investigadores dijeron a ZDNet que creen que el falso descargador se distribuye por medio de correos electrónicos de phishing enviados masivamente a objetivos potenciales, ya que esta es históricamente la forma más común de comenzar los ataques de LokiBot.

La descarga y ejecución del falso lanzador de Epic Games, que utiliza el logotipo de la compañía para parecer legítimo, inicia el proceso de infección. Esto comienza con el malware que deja caer dos archivos separados, un archivo de código fuente C# y un ejecutable .NET, en el directorio de datos de la aplicación de la computadora.

El código fuente de C# está muy ofuscado, y contiene porciones de código basura que no significan nada, pero que permiten que el instalador de LokiBot omita cualquier medida de seguridad en la máquina.

Una vez dentro del sistema, el archivo .NET lee y cumple el código C#, antes de descifrarlo y ejecutar LokiBot en una máquina infectada. Esto le proporciona al atacante la puerta trasera necesaria para robar información, monitorear actividad, instalar otro malware y llevar a cabo otras acciones maliciosas.

A pesar de tener cinco años, LokiBot sigue siendo una amenaza de malware prolífica, en parte porque al inicio de su vida, el código subyacente se filtró, lo que brinda a los delincuentes cibernéticos la oportunidad de desarrollar sus propias versiones del malware. Esto podría venderse en foros subterráneos como servicio, para que los hackers de bajo nivel lo utilicen en sus propios ataques.

Esta última versión de LokiBot sugiere que el malware seguirá siendo una amenaza por algún tiempo.

> *«Constantemente entre los infostealers más activos en la naturaleza, estos ajustes a su instalación y mecanismos de ofuscación indican que LokiBot no va a reducir la velocidad en un futuro próximo»,* dijeron los investigadores de Trend Micro.