Se descubrió una versión PHP de una malware de robo de información llamado Ducktail, que se distribuye en forma de instaladores descifrados para aplicaciones y juegos legítimos, según los últimos hallazgos de Zscaler.

> *«Al igual que las versiones anteriores (.NetCore), la última versión (PHP) también tiene como objetivo extraer información confidencial relacionada con las credenciales guardadas del navegador, la información de la cuenta de Facebook, etc.»*, dijeron los investigadores de Zscaler ThreatLabz, Tarun Dewan y Stuti Chaturvedi.

Ducktail, que surgió en el panorama de amenazas a fines de 2021, se atribuye a un actor de amenazas vietnamieta no identificado, con el malware diseñado principalmente para secuestrar cuentas comerciales y publicitarias de Facebook.

La operación cibercriminal con motivación financiera fue documentada por primera vez por la compañía finlandesa de seguridad cibernética WithSecrure (antes F-Secure) a finales de julio de 2022.

Aunque se descubrió que las versiones anteriores del malware usaban Telegram como un canal de comando y control (C2) para filtrar información, la variante de PHP detectada en agosto de 2022 establece conexiones a un sitio web recién alojado para almacenar los datos en formato JSON.

Las cadenas de ataque observadas por Zscaler implican incrustar el malware en archivos ZIP alojados en servicios de intercambio de archivos como mediafire[.]com, haciéndose pasar por versiones descifradas de Microsoft Office, juegos y archivos relacionados con material pornográfico.

La ejecución del instalador, a su vez, activa un script PHP que, en última instancia, inicia el código responsable de robar y extraer datos de los navegadores web, las billeteras de criptomonedas y las cuentas de Facebook Business.

> *«Parece que los actores de amenazas detrás de la campaña del ladrón Ducktail están continuamente haciendo cambios o mejoras en los mecanismos de entrega y el enfoque para robar una amplia variedad de información confidencial del usuario y del sistema dirigida a los usuarios en general»,* dijeron los investigadores.