Se ha observado una nueva campaña de malware que usa información confidencial robada de un banco como señuelo en correos electrónicos de phishing para lanzar un troyano de acceso remoto llamado BitRAT.

Se cree que el atacante desconocido secuestró la infraestructura de TI de un banco cooperativo colombiano y usó la información para crear mensajes de señuelo convincentes para atraer a las víctimas para que abran archivos adjuntos de Excel sospechosos.

El descubrimiento proviene de la compañía de seguridad cibernética Qualys, que encontró evidencia de un volcado de base de datos que comprende 418,777 registros que se dice que se obtuvieron al explotar las vulneraiblidades de inyección de SQL.

Los detalles filtrados incluyen números de cédula (un documento nacional de identidad emitido a los ciudadanos colombianos), direcciones de correo electrónico, números de teléfono, nombres de clientes, registros de pago, detalles de salarios y direcciones, entre otros.

No existen indicios de que la información se haya compartido previamente en ningún foro de la red oscura o normal, lo que sugiere que los mismos actores de amenazas obtuvieron acceso a los datos de los clientes para montar los ataques de phishing.

El archivo de Excel, que contiene los datos bancarios extraídos, también incorpora una macro que se usa para descargar una carga útil de DLL de segunda etapa, que está configurada para recuperar y ejecutar BitRAT en el host comprometido.

> *«Utiliza la biblioteca WinHTTP para descargar cargas útiles integradas de BitRAT desde GitHub al directorio %temp%»,* dijo Akshat Pradhan, investigador de Qualys.

Creado a mediados de noviembre de 2022, el repositorio de GitHub se usa para alojar muestras ofuscadas del cargador BitRAT que finalmente se decodifican y lanzan para completar las cadenas de infección.

BitRAT, un malware estándar disponible a la venta en foros clandestinos por solo $20 dólares, viene con una amplia gama de funcionalidades para robar datos, recolectar credenciales, extraer criptomonedas y descargar binarios adicionales.

> *«Los RAT comerciales disponibles han estado evolucionando su metodología para propagarse e infectar a sus víctimas. También han aumentado el uso de infraestructuras legítimas para alojar sus cargas útiles y los defensores deben dar cuenta de ello»,* dijo Pradhan.