ESET descubre un nuevo troyano bancario que ataca a usuarios corporativos en Brasil

El equipo de investigación de **ESET** ha descubierto un **troyano bancario** que se dirige a usuarios corporativos en Brasil desde, al menos, 2019. **Janeleiro** (como han denominado al troyano) afecta a sectores como la ingeniería, medicina, comercio minorista, manufactura, finanzas, transporte e instituciones gubernamentales.

El engaño se lleva a cabo mediante **ventanas emergentes** diseñadas para parecerse a los sitios web de algunos de los bancos más grandes de Brasil. Después, pretende que los usuarios **ingresen sus credenciales bancarias e información personal**. En todo este proceso, el troyano controla las ventanas en pantalla, elimina crhome.exe, realiza capturas de pantalla, envía información sobre los clicks del ratón, graba la pantalla en tiempo real y puede secuestrar el portapapeles para cambiar las direcciones de bitcoin con las de los criminales a tiempo real.

Janeleiro sigue el mismo plan para su implementación central que muchas otras **familias de malware** que tienen como objetivo Brasil. Aunque se distingue de ellas en varios aspectos, como el lenguaje de codificación.

“La naturaleza de un ataque de Janeleiro no se caracteriza por sus capacidades de automatización, sino más bien por el enfoque práctico: en muchos casos, el operador debe ajustar las ventanas emergentes mediante comandos ejecutados en tiempo real”, dice el investigador de ESET**, Facundo Muñoz, quien descubrió a Janeleiro**.

“Parece que el troyano bancario estaba **en desarrollo ya en 2018**, y en 2020 mejoró su procesamiento de comandos para darle al operador un mejor control durante el ataque”, agrega Muñoz, quien continúa: “La naturaleza experimental de Janeleiro, yendo y viniendo entre diferentes versiones, nos habla de un actor que todavía está tratando de encontrar la mejor manera de llevar adelante su objetivo, pero esto no quiere decir que tiene menos experiencia que la competencia: Janeleiro sigue el mismo modelo para la implementación del núcleo de las ventanas emergentes falsas como muchos troyanos bancarios de LATAM, esto no parece ser una coincidencia o inspiración: este actor emplea y distribuye Janeleiro compartiendo la misma infraestructura que algunas de las familias de malware activas más prominentes”.