¿Qué tipo de amenaza es?

Es un troyano llamado “Janeleiro”.

¿Cómo comienza y cómo se propaga esta amenaza?

Esta amenaza se propaga por mail, mediante la técnica de phishing. El ataque comienza con un correo electrónico de phishing que pretende ser una factura impaga, que contiene un enlace que, cuando se hace clic, descarga un archivo ZIP. El archivo viene con un instalador MSI que carga la DLL del troyano principal, que posteriormente obtiene las direcciones IP de los servidores de comando y control (C2) de una página de GitHub aparentemente creada por los autores del malware. El último eslabón de la cadena de infección implica la espera de comandos del servidor C2. Así, en el caso de que un usuario visite el sitio web de una entidad bancaria de interés, Janeleiro se conecta al servidor C2 y muestra dinámicamente las ventanas emergentes fraudulentas, y captura las pulsaciones de teclas y otra información ingresada en los formularios falsos.

¿Hay más de una amenaza aplicada?

No, solo el troyano.