Falso correo electrónico de WhatsApp descarga troyano bancario

ESET, compañía líder en detección proactiva de amenazas, advierte sobre un falso correo electrónico en español que intenta hacer creer a las potenciales víctimas que se trata de una comunicación oficial de WhatsApp que invita a descargar una copia de seguridad de las conversaciones y el historial de llamadas en la aplicación de mensajería.

El objetivo real de la comunicación es distribuir el troyano bancario Grandoreiro, que roba credenciales bancarias mediante ventanas emergentes falsas que hacen creer a la víctima que se trata del sitio oficial del banco, entre otras funcionalidades.

Pie de imagen: La Oficina de Seguridad del Internauta de España (OSI) y la Guardia Civil alertaron acerca de una campaña de phishing en la cual se intenta suplantar la identidad de WhatsApp: Correo que ha estado circulando e incluye un archivo HTML adjunto. Fuente: OSI.

En el correo que suplanta la identidad de WhatsApp, el mensaje incluye un archivo adjunto nombrado “Open_Document_513069.html”. Se trata de un archivo HTML que contiene una URL acortada mediante el servicio bitly. Según un análisis realizado en el laboratorio de ESET Latinoamérica del HTML adjunto, al hacer clic redirecciona a un sitio desde el cual se descarga un archivo .zip. Ese archivo comprimido contiene un instalador MSI que descarga la amenaza, el troyano bancario Grandoreiro. Si el usuario ejecuta el archivo descargado, probablemente el equipo haya sido infectado con el malware.

Según análisis detallado de Grandoreiro que publicó ESET, se trata de un troyano bancario escrito en Delphi que comparte muchas características con otras familias de troyanos muy activas en América Latina. Algunas de estas familias, se expandieron más allá de Latinoamérica y comenzaron a dirigir sus campañas a usuarios de España y de otros países de Europa. En 2020, Grandoreiro tenía presencia principalmente en países como Brasil, España, México y Perú. Y a poco de decretarse la pandemia se detectaron correos en los que utilizó la temática del COVID-19 para engañar a los usuarios, así como campañas dirigidas a España suplantando la identidad de la Agencia

Tributaria.

Una vez que infectó el equipo de la víctima, el objetivo principal de este troyano es robar credenciales bancarias mediante ventanas emergentes falsas que hacen creer a la víctima que se trata del sitio oficial del banco. Además, al igual que los otros troyanos bancarios latinoamericanos, cuenta con funcionalidades de backdoor que le permiten al atacante realizar otras acciones maliciosas en el equipo comprometido, como registras las pulsaciones de teclado (keylogging), simular acciones de mouse y teclado, cerrar sesión de la víctima, bloquear el acceso a ciertos sitios o incluso reiniciar el equipo, por nombrar algunas de sus capacidades.

De acuerdo con los datos de la telemetría de ESET, los registros de los últimos 90 días para la misma variante de Grandoreiro detectada en esta campaña que suplanta la identidad de WhatsApp muestran actividad del troyano en España principalmente, pero también en México y Brasil. “Esto no quiere decir que sea la misma campaña esté circulando en estos países, pero tampoco podemos descartar la posibilidad de que esta misma estrategia de ingeniería social no se utilice más adelante en campañas que apunten a países de América Latina, por lo que es importante estar informado de este tipo de campañas de phishing para evitar caer en la trampa en caso de recibir un correo de estas características.”, comenta Camilo Gutiérrez Amaya, Jefe de Laboratorio de Seguridad Informática de ESET Latinoamérica.

Desde el sitio de la Oficina de Seguridad del Internauta no descartan que existan otros correos en circulación con asuntos diferentes. De hecho, en marzo de este año estuvo circulando en España una campaña de phishing de similares características en la cual se suplantaba la identidad de WhatsApp utilizando la misma excusa, y también hay registros de una campaña similar en 2020.

Con información de El Impulso