Kaspersky Lab informó sobre una operación cibernética denominada Dark Tequila, que ha estado atacando a usuarios en México durante al menos cinco años, robando credenciales bancarias y datos personales por medio de un código malicioso.

Según la firma de ciberseguridad, la operación de los hackers cuenta con la particularidad de moverse de forma lateral por medio de las computadoras de las víctimas sin conexión a Internet.

> *«Según los investigadores de Kaspersky Lab, el código malicioso se propaga a través de dispositivos USB infectados y de spear-phishing, incluyendo funcionalidades especiales para evadir la detección. Se cree que el agente de amenaza detrás de Dark Tequila es de origen hispanohablante y latinoamericano»,* explica la empresa.

Kaspersky destacó en su estudio que el malware Dark Tequila y su infraestructura de apoyo son inusualmente avanzados para las operaciones de fraude financiero.

> *«La amenaza se centra, principalmente, en robar la información financiera, pero una vez dentro de una computadora, también sustrae credenciales de otras páginas, incluso sitios web populares, recolectando direcciones corporativas y personales de correo electrónico, cuentas de registros de dominio, de almacenamiento de archivos y más, posiblemente para ser vendidas o usadas en operaciones futuras»,* agregó.

Kaspersky detalla que el malware lleva una carga útil de distintas etapas e infecta los dispositivos de usuarios por medio de USB infectados y correos electrónicos de phishing. Una vez dentro de una computadora, el malware se comunica con su servidor de mandos para recibir instrucciones.

> *«La carga útil se entrega a la víctima sólo cuando se cumplen ciertas condiciones. Si el malware detecta que existe una solución de seguridad instalada, monitoreo de red o signos de que la muestra se ejecuta en un entorno de análisis, detiene su rutina de infección y se auto-elimina del sistema»,* explica Kaspersky.

De este modo, si el código malicioso no encuentra ninguna de las condiciones anteriores, el malware activa la infección y copia un archivo ejecutable en una unidad extraíble para que se ejecute de forma automática.

> *«Esto permite que el malware se traslade por medio de la red de la víctima, aunque no esté conectada a Internet o incluso cuando la red tiene varios segmentos no conectados entre sí. Cuando se conecta otro USB a la computadora infectada, este se infecta de forma automática para así poder infectar otro objetivo, cuando mismo USB sea conectado»,* agregó.