El grupo de hackers conocido como Blind Eagle, ha sido vinculado a una nueva campaña dirigida a varias industrias clave en Colombia.

También se cree que la actividad, que fue detectada por el equipo de investigación e inteligencia de BlackBerry el 20 de febrero de 2023, abarca Ecuador, Chile y España, lo que sugiere una lenta expansión de la huella de victimología del grupo de hackers.

Las entidades objetivo incluyen salud, finanzas, aplicación de la ley, inmigración y una agencia a cargo de las negociaciones de paz en Colombia, dijo la compañía canadiense de seguridad.

Blind Eagle, también conocido como APT-C-36, fue descubierto recientemente por Check Point Research, que detalla el conjunto de herramientas avanzadas del adversario que comprende las cargas útiles de Meterpreter que se entregan por medio de correos electrónicos de phishing.

El último conjunto de ataques involucra al grupo que se hace pasar por la agencia tributaria del gobierno colombiano, la Dirección Nacional de Impuestos y Aduanas (DIAN), para phishing a sus objetivos usando señuelos que instan a los destinatarios a liquidar *«obligaciones pendientes».*

Los mensajes de correo electrónico ingeniosamente diseñados cuentan con un enlace que apunta a un archivo PDF que supuestamente está alojado en el sitio web de DIAN, pero en realidad implementa malware en el sistema objetivo, iniciando efectivamente la cadena de infección.

> *«La página falsa del sitio web de la DIAN contiene un botón que alienta a la víctima a descargar un PDF para ver lo que el sitio web afirma que son facturas de impuestos pendientes»,* dijeron los investigadores de BlackBerry.

> *«Al hacer clic en el botón azul se inicia la descarga de un archivo malicioso de la red de entrega de contenido (CDN) de Discord, que los atacantes están abusando en esta estafa de phishing».*

La cara útil es un Visual Basic Script (VBS), que se ejecuta al abrir el archivo «PDF» y usa PowerShell para recuperar un archivo DLL basado en .NET que finalmente carga AsyncRAT en la memoria.

> *«El troyano de acceso remoto malicioso instalado en la máquina de una víctima permite que el actor de amenazas se conecte al punto final infectado en cualquier momento y realice las operaciones que desee»*, dijeron los investigadores.

También cabe mencionar el uso que hace el atacante de servicios de DNS dinámicos como DuckDNS para controlar remotamente los hosts comprometidos.

Se sospecha que Blind Eagle es un grupo de habla hispana debido al uso del idioma en sus correos electrónicos de spear-phishing. Sin embargo, actualmente no está claro dónde se encuentra el actor de la amenaza y si sus ataques están motivados por espionaje o por ganancias económicas.

> *«El modus operandi utilizado en su mayoría se ha mantenido igual que los esfuerzos anteriores del grupo: es muy simple, lo que puede significar que este grupo se siente cómodo con su forma de lanzar campañas a través de correos electrónicos de phishing y confía en usarlos porque siguen trabajando»,* dijo BlackBerry.