Investigadores en ciberseguridad han revelado información sobre un grupo de amenazas conocido como Blind Eagle, que ha estado atacando de manera constante a organizaciones e individuos en Colombia, Ecuador, Chile, Panamá y otros países de América Latina.

Los objetivos de estos ataques incluyen varios sectores, como instituciones gubernamentales, empresas financieras, compañías energéticas y del sector petrolero.

> *«Blind Eagle ha mostrado capacidad para adaptar sus ciberataques según sus objetivos y la versatilidad para alternar entre ataques con fines financieros y operaciones de espionaje»*, señaló Kaspersky en un informe publicado el lunes.

También conocido como APT-C-36, se cree que Blind Eagle está activo desde al menos 2018. Este grupo, que se sospecha es de habla hispana, es conocido por emplear señuelos de spear-phishing para distribuir varios troyanos de acceso remoto disponibles públicamente, como AsyncRAT, BitRAT, Lime RAT, NjRAT, Quasar RAT y Remcos RAT.

A principios de marzo, eSentire detalló cómo este grupo utilizó un cargador de malware llamado Ande Loader para propagar Remcos RAT y NjRAT.

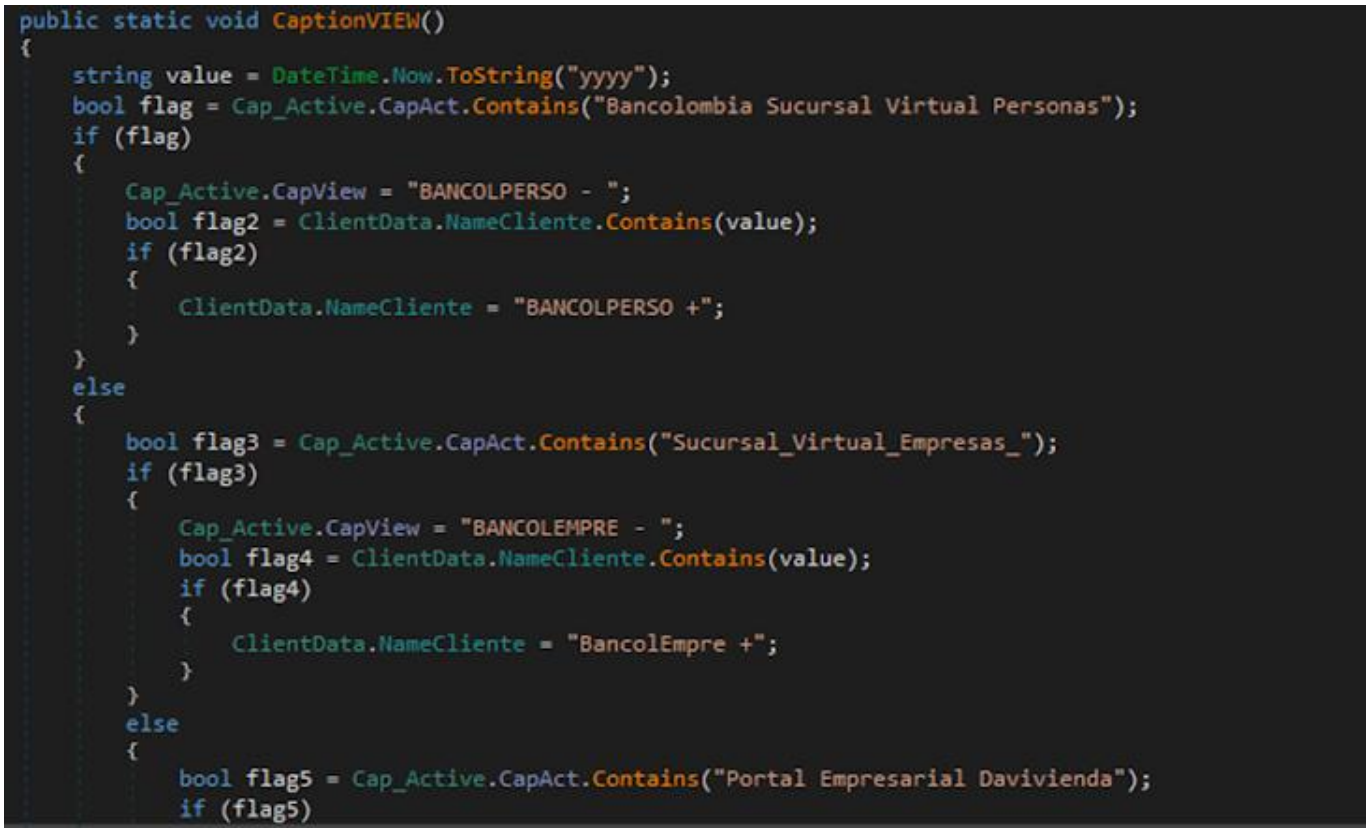
El ataque comienza con un correo electrónico de phishing que se hace pasar por instituciones gubernamentales legítimas y entidades financieras o bancarias, advirtiendo a los destinatarios que deben tomar medidas urgentes haciendo clic en un enlace que supuestamente los llevará al sitio web oficial de la entidad imitada.

Estos correos electrónicos también incluyen un archivo adjunto en formato PDF o Microsoft Word que contiene la misma URL y, en algunos casos, algunos detalles adicionales diseñados para aumentar el sentido de urgencia y hacer que el mensaje parezca más legítimo.

El primer conjunto de URLs dirige a los usuarios a sitios web controlados por los atacantes que alojan un dropper inicial, pero solo después de verificar si la víctima pertenece a uno de los países objetivo del grupo. De lo contrario, son redirigidos al sitio web real de la

organización que los atacantes están suplantando.

> *«Esta redirección geográfica impide que los nuevos sitios maliciosos sean detectados y complica la caza y el análisis de estos ataques»,* explicó la empresa de ciberseguridad rusa.



```
public static void CaptionVIEW()
{
    string value = DateTime.Now.ToString("yyyy");
    bool flag = Cap_Active.CapAct.Contains("Bancolombia Sucursal Virtual Personas");
    if (flag)
    {
        Cap_Active.CapView = "BANCOLPERSO - ";
        bool flag2 = ClientData.NameCliente.Contains(value);
        if (flag2)
        {
            ClientData.NameCliente = "BANCOLPERSO +";
        }
    }
    else
    {
        bool flag3 = Cap_Active.CapAct.Contains("Sucursal_Virtual_Empresas_");
        if (flag3)
        {
            Cap_Active.CapView = "BANCOLEMPRE - ";
            bool flag4 = ClientData.NameCliente.Contains(value);
            if (flag4)
            {
                ClientData.NameCliente = "BancolEmpre +";
            }
        }
        else
        {
            bool flag5 = Cap_Active.CapAct.Contains("Portal Empresarial Davivienda");
            if (flag5)
```

El dropper inicial se presenta como un archivo comprimido en formato ZIP, que contiene un script de Visual Basic (VBS) encargado de descargar la siguiente etapa de la carga maliciosa desde un servidor remoto predeterminado. Estos servidores pueden incluir desde sitios de alojamiento de imágenes hasta plataformas como Pastebin o servicios legítimos como Discord y GitHub.

El malware de segunda etapa, a menudo oculto mediante técnicas de esteganografía, es un archivo DLL o un inyector .NET que luego se conecta a otro servidor malicioso para descargar el troyano final.

> *«El grupo suele utilizar técnicas de inyección de procesos para ejecutar el RAT en la memoria de un proceso legítimo, eludiendo así las defensas basadas en procesos»*, indicó Kaspersky.
>
> *«La técnica preferida por el grupo es el proceso hollowing. Esta técnica implica crear un proceso legítimo en estado suspendido, luego desmapear su memoria, reemplazarla con una carga maliciosa y finalmente reanudar el proceso para iniciar la ejecución.»*

El uso de versiones modificadas de RATs de código abierto le da a Blind Eagle la capacidad de ajustar sus campañas a conveniencia, utilizándolas para ciberespionaje o para capturar credenciales de servicios financieros en Colombia desde el navegador de la víctima, cuando los títulos de las ventanas coinciden con una lista predefinida de cadenas en el malware.

Por otro lado, se han observado versiones alteradas de NjRAT con capacidades para registrar teclas y capturar pantallas, lo que permite recolectar información sensible. Además, la versión actualizada permite instalar plugins adicionales enviados desde un servidor para aumentar su funcionalidad.

Las modificaciones también se extienden a las cadenas de ataque. Tan recientemente como en junio de 2024, AsyncRAT ha sido distribuido a través de un cargador de malware llamado Hijack Loader, lo que demuestra un alto grado de adaptabilidad por parte de los atacantes. Esto también resalta la incorporación de nuevas técnicas para mantener sus operaciones activas.

> *«Aunque las técnicas y procedimientos de Blind Eagle puedan parecer simples, su efectividad permite al grupo mantener un alto nivel de actividad. Al ejecutar continuamente campañas de ciberespionaje y robo de credenciales financieras, Blind Eagle sigue siendo una amenaza significativa en la región»,* concluyó Kaspersky.