Informe

Seguimiento a la actividad del actor APT-C-36

COLCERT IN-20260209-028

TIC

TLP:CLEAR

Resumen Ejecutivo

El presente informe analiza la actividad del actor de amenazas **APT-C-36**, también conocido como **Blind Eagl**e o **TAG-144**, un grupo activo y persistente en el panorama de ciberamenazas que afecta a Colombia y América Latina. Este actor se caracteriza por campañas sostenidas de phishing dirigido, diseñadas específicamente para explotar debilidades en la infraestructura tecnológica de entidades de gobierno colombianas,.

El análisis evidencia que APT-C-36 posee un alto grado de especialización regional, reflejado en el uso de señuelos que suplantan entidades estatales como la DIAN, la Rama Judicial, la Fiscalía General de la Nación y otras instituciones oficiales. Estas campañas generan una sensación de urgencia y autoridad que incrementa la probabilidad de interacción por parte de las víctimas, facilitando el acceso inicial a los sistemas comprometidos.

Desde el punto de vista técnico, el grupo emplea cadenas de infección multi-etapa, combinando enlaces maliciosos, archivos HTML/SVG, ejecutables disfrazados y técnicas de evasión orientadas a reducir la detección temprana. En campañas recientes se ha observado el despliegue de troyanos de acceso remoto (RAT), como **AsyncRAT** o **XWorm**, configurado de forma estática y con capacidades completas de control remoto, vigilancia del usuario, exfiltración de información y comunicación cifrada con infraestructura de comando y control (C2).

En conjunto, **APT-C-36** representa una amenaza relevante y continua para el ecosistema digital colombiano, especialmente para entidades públicas con alta dependencia del correo electrónico y procesos administrativos digitalizados. Su persistencia operativa, conocimiento del entorno local y adaptación constante subrayan la necesidad de fortalecer la detección temprana, la concienciación del personal y el monitoreo de tráfico e infraestructura, así como de mantener una vigilancia activa frente a este actor y sus campañas emergentes.

Introducción

El grupo de amenazas conocido como **ATP-C-36**, también identificado en diferentes reportes como **Blind Eagle**, **ÁguilaCiega**, **APT-Q-98** y **TAG-144**, es un actor de amenazas persistente avanzada (APT) activo desde al menos 2018. Este grupo se caracteriza por el uso sistemático de campañas de *phishing* dirigidas como principal vector de acceso inicial, con el objetivo de comprometer sistemas, recolectar credenciales y desplegar herramientas de acceso remoto.

Sus operaciones se concentran en América Latina, con un énfasis sostenido en Colombia, donde ha dirigido múltiples campañas contra entidades gubernamentales, instituciones públicas y sectores estratégicos. Adicionalmente, se han observado actividades relacionadas en países como Ecuador, Chile y Panamá, lo que evidencia un interés regional con objetivos institucionales y administrativos.

A lo largo de los años, el grupo ha demostrado una evolución constante de sus tácticas, combinando ingeniería social con el uso de infraestructura legítima para la distribución de *malware*, como servicios de almacenamiento en la nube y repositorios públicos. Entre las herramientas más utilizadas se encuentran distintos troyanos de acceso remoto (RAT), empleados para el control de sistemas comprometidos y la exfiltración de información sensible.

Cyber Kill Chain

Reconocimiento

APT-C-36 realiza una recolección de información sobre sus objetivos, la identificación de direcciones de correo institucionales y la elaboración de los señuelos alineados con procesos administrativos reales.

Se preparan los elementos necesarios para la campaña, diseñando archivos y enlaces maliciosos que simulan documentos legítimos.

Preparación

Entrega

La entrega del contenido malicioso se realiza por medio de correos electrónicos de phishing. Estos mensajes suelen contener botones o enlaces que invitan a descargar documentos relevantes para la víctima.

Se inicia mediante la interacción del usuario, generalmente haciendo clic en un enlace o archivo adjunto en el correo electrónico malicioso. Esta acción desencadena la descarga de componentes adicionales desde infraestructura remota.

Explotación

Instalación

Tras la descarga exitosa, se instala en el sistema operativo un troyano de acceso remoto (RAT), proporcionando al grupo APT-C-36 el control persistente en el equipo comprometido.

La muestra establece comunicación con la infraestructura de comando y control (C2), utilizando protocolos de red y en algunos casos, servicios legítimos para camuflar el tráfico malicioso dentro de comunicaciones normales

Comando y Control

Acciones sobre el objetivo

La muestra establece comunicación con la infraestructura de comando y control (C2), utilizando protocolos de red y en algunos casos, servicios legítimos para camuflar el tráfico malicioso dentro de comunicaciones normales

Vector de ataque

Las campañas de **APT-C-36** exhiben un alto grado de especialización regional, diseñadas para explotar debilidades de entidades publicas A diferencia de actores globales que traducen plantillas genéricas, este grupo demuestra un conocimiento profundo de la burocracia colombiana, utilizando terminología precisa y formatos oficiales convincentes.

El vector de ataque predominante se basa en la suplantación de identidad de entidades estatales, generando una sensación de urgencia en la víctima, se han identificado campañas masivas suplantando a:

- **DIAN (Dirección de Impuestos y Aduanas Nacionales):** correos sobre supuestos "procesos de cobro coactivo", "embargos de cuentas bancarias" o "facturación electrónica obligatoria". Es la temática más recurrente debido a su impacto directo sobre empresas y ciudadanos.

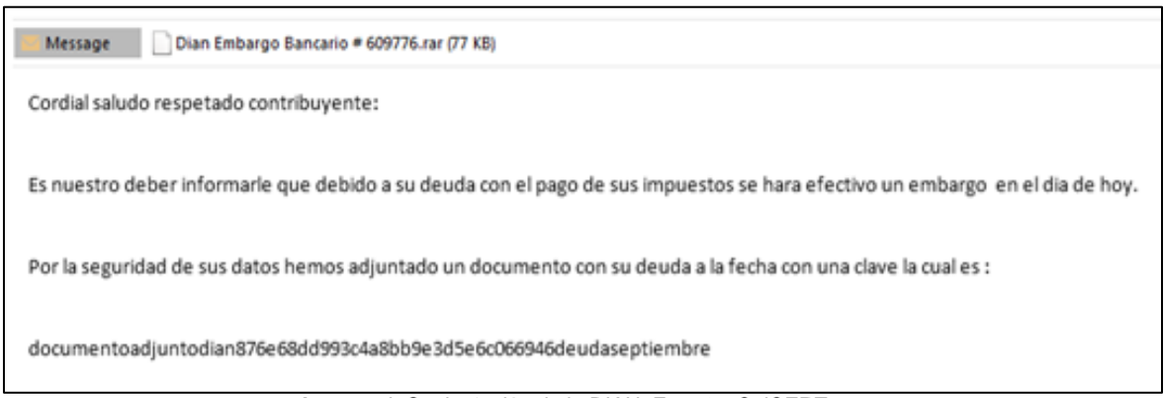

Imagen 1. *Suplantación de la DIAN.* ***Fuente:*** *ColCERT.*

- **Rama Judicial y Fiscalía General de la Nación:** notificaciones falsas de "citaciones a audiencia", "demandas en curso" o "apertura de procesos penales". Estos señuelos suelen incluir supuestos enlaces a expedientes digitales.

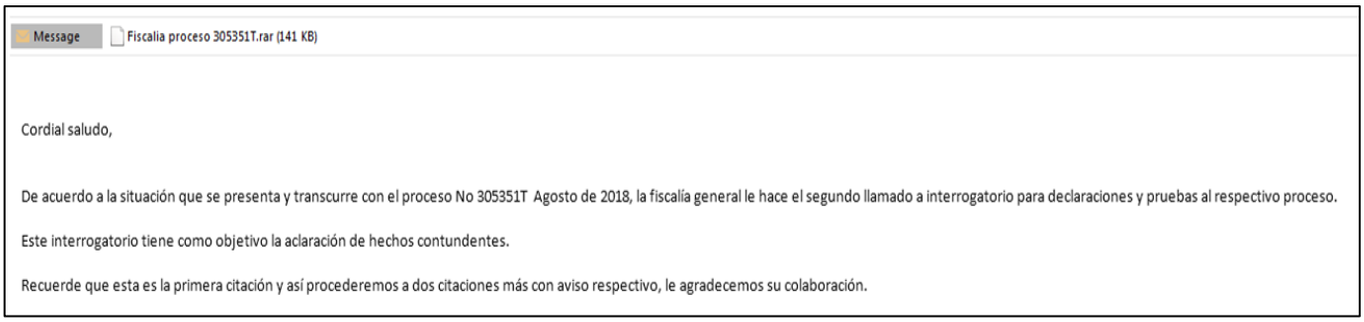

Imagen 2. *Suplantación de la Fiscalía General de la Nación.* ***Fuente:*** *ColCERT.*

- **Centro Cibernético Policial y Cancillería:** en menor medida, se han detectado campañas relacionadas con antecedentes judiciales o trámites de pasaportes.

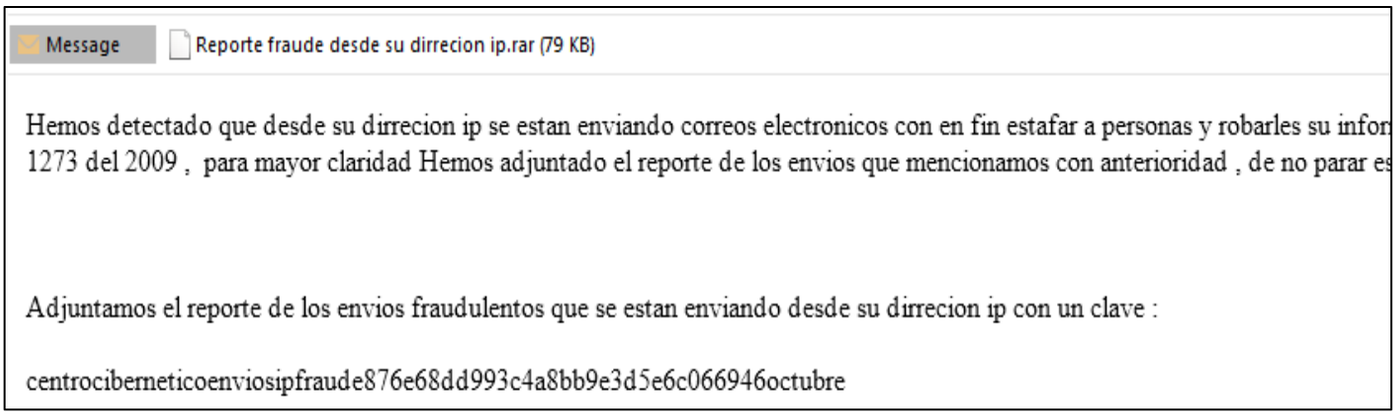

Imagen 3. *Suplantación del Centro Cibernético Policial.* ***Fuente:*** *ColCERT.*

Una vez establecida la interacción inicial mediante el engaño, la cadena de infección puede continuar a través de múltiples mecanismos de entrega de *malware*, los cuales varían entre campañas pero mantienen patrones consistentes orientados a evadir controles de seguridad.

- **Enlaces maliciosos (URL):** los correos pueden contener archivos URL, botones o hipervínculos que redirigen a sitios controlados por el atacante o a recursos alojados en servicios legítimos (cloud, repositorios de archivos), desde donde se descarga la siguiente etapa del ataque. Esta técnica permite evadir filtros de correo que priorizan la inspección de adjuntos.

- **Archivos HTML o SVG maliciosos:** se han observado campañas que emplean archivos HTML o SVG que simulan documentos oficiales. Al ser abiertos, estos archivos ejecutan código embebido que redirige al usuario a una infraestructura remota o descarga automáticamente cargas adicionales. En algunos casos, los archivos SVG han sido utilizados como contenedores para ofuscar enlaces o scripts maliciosos.

- **Documentos con macros o scripts embebidos:** aunque en menor proporción que en campañas anteriores, el grupo continúa utilizando documentos ofimáticos que requieren habilitar contenido activo, lo que facilita la ejecución de scripts encargados de descargar y ejecutar el malware final.

- **Ejecutables maliciosos disfrazados:** la cadena puede culminar en la descarga de archivos ejecutables que se presentan como archivos PDF, comprobantes o documentos escaneados, aprovechando extensiones dobles o iconografía engañosa para inducir su ejecución.

- **Técnicas de esteganografía:** en campañas más sofisticadas, se ha documentado el uso de imágenes aparentemente benignas que contienen datos maliciosos ocultos. Estas imágenes son descargadas durante etapas intermedias y posteriormente procesadas por scripts o loaders para extraer y ejecutar la carga final.

Imagen 4. *Técnicas para la entrega de la carga maliciosa: ColCERT.*

Independientemente del mecanismo específico, el objetivo de esta fase es entregar e instalar una herramienta de acceso remoto que permita al atacante mantener persistencia y control del sistema comprometido.

Análisis estático

Se realizó el análisis de una muestra de **AsyncRAT** con hash MD5 “885127590b2c7ec029e1c5aab5d0635a”, la cual fue utilizada en campañas del grupo **APT-C-36** y que para efectos de estudio fue renombrada localmente como “**AsyncRAT.exe**”, para su ejecución en un ambiente controlado y su trazabilidad en registros y artefactos generados durante las pruebas.

Los metadatos pertenecientes a la muestra analizada son los siguientes:

Información de la muestra analizada AsyncRAT.exe	
MD5	885127590b2c7ec029e1c5aab5d0635a
SHA1	a74100abab8962b0cdc97bedb9399180443c0f3e
SHA256	8e1f62b87234e54baf7ca40bfd2a81a6ed53b5a009b15ce7e4cba7d54d39a3a2
SSDEEP	1536:FmIm86tX2kNff4sKu+UYFDGXw5bfAPGBKB4ic/drQTGZx:Fm986tmkN7Ku+UYFDGXw5bfKBLc/dGix
Nombre del archivo	AsyncRAT.exe
Tipo de archivo	Win32 EXE
Tamaño	63.00 KB (64512 bytes)

Tabla 1. *Metadatos de la muestra: ColCERT.*

Durante el análisis estático de la muestra se identificó que corresponde a un ejecutable PE32 (i386, 32-bit) para sistemas Windows, con subsistema GUI, lo que indica que el binario no presenta una interfaz de consola visible para el usuario y busca ejecutarse de forma discreta. El archivo fue enlazado utilizando Microsoft Linker 8.0 y compilado en VB.NET, apoyándose en librerías de .NET Framework v4.6 (CLR v4.0.30319), una característica común en variantes modernas de **AsyncRAT** debido a la flexibilidad que ofrece el entorno .NET para la ofuscación y carga dinámica de componentes.

Imagen 5. *Detalle metadatos de AsyncRAT: ColCERT.*

Análisis estático

Durante el análisis estático de la muestra se identificaron **74** funciones importadas marcadas como potencialmente maliciosas, asociadas principalmente a capacidades de captura de información, evasión y comunicación en red. La concentración y diversidad de estas funciones evidencian que el binario no cumple un propósito legítimo único, sino que integra múltiples módulos orientados al control remoto del sistema comprometido, característica típica de herramientas RAT como **AsyncRAT**. La presencia de llamadas directas a API del sistema operativo, combinadas con clases del framework .NET relacionadas con red, criptografía y seguridad, refuerzan la hipótesis de una herramienta diseñada para operar de forma persistente y sigilosa. A continuación, las más relevantes:

- **SetWindowsHookEx / CallNextHookEx (user32.dll):** permiten instalar hooks a nivel del sistema para interceptar eventos de teclado y mouse. Su presencia indica capacidades de monitoreo continuo de la actividad del usuario, comúnmente asociadas a *keylogging* y vigilancia encubierta.

- **GetKeyState / GetKeyboardState (user32.dll):** funciones utilizadas para capturar el estado de las teclas presionadas. Estas llamadas confirman la capacidad del malware para registrar credenciales y otra información sensible ingresada por la víctima.

- **Socket / NetworkStream (System.Net.Sockets):** constituyen la base de la comunicación de red del malware, permitiendo establecer sesiones persistentes con servidores de Comando y Control (C2) y facilitar la exfiltración de datos.

- **WebClient / DownloadFile (System.Net):** permiten la descarga dinámica de cargas adicionales, lo que habilita la actualización del malware, la entrega de nuevos módulos o la adaptación de la campaña sin requerir una nueva infección inicial.

- **SslStream / RemoteCertificateValidationCallback (System.Net.Security):** indican el uso de canales de comunicación cifrados, potencialmente con validaciones de certificados relajadas, lo que dificulta la inspección del tráfico y favorece la evasión de controles de red.

- **X509Certificate / RSACryptoServiceProvider (System.Security.Cryptography):** componentes criptográficos utilizados para cifrar comunicaciones y datos exfiltrados, así como para proteger configuraciones internas del malware, alineados con técnicas de ofuscación y protección de información.

imports (691)	namespace (34)	flag (74)	callback (0)	group (15)	technique (11)	type (2)	ordinal (0)	library (5)
GetForegroundWindow	-	x	-	windowing	T1010 | Window Discovery	P/Invoke	-	user32.dll
GetWindowText	-	x	-	windowing	T1010 | Window Discovery	P/Invoke	-	user32.dll
SslProtocols	System.Security.Authenticat...	x	-	security	-	TypeRef	-	mscoree.dll
WindowsIdentity	System.Security.Principal	x	-	security	-	TypeRef	-	mscoree.dll
WindowsPrincipal	System.Security.Principal	x	-	security	-	TypeRef	-	mscoree.dll
WindowsBuiltInRole	System.Security.Principal	x	-	security	-	TypeRef	-	mscoree.dll
GetEnvironmentVariable	-	x	-	reconnaissance	-	MemberRef	-	mscoree.dll
Decompress	-	x	-	obfuscation	-	Method	-	mscoree.dll
Compress	-	x	-	obfuscation	-	Method	-	mscoree.dll
DownloadFile	-	x	-	network	T1086 | PowerShell	MemberRef	-	mscoree.dll
Socket	System.Net.Sockets	x	-	network	-	TypeRef	-	mscoree.dll
SslStream	System.Net.Security	x	-	network	-	TypeRef	-	mscoree.dll
SslPolicyErrors	System.Net.Security	x	-	network	-	TypeRef	-	mscoree.dll
IPAddress	System.Net	x	-	network	T1011 | Network Exfiltration	TypeRef	-	mscoree.dll
WebClient	System.Net	x	-	network	T1011 | Network Exfiltration	TypeRef	-	mscoree.dll
NetworkCredential	System.Net	x	-	network	T1011 | Network Exfiltration	TypeRef	-	mscoree.dll
AddressFamily	System.Net.Sockets	x	-	network	-	TypeRef	-	mscoree.dll
SocketType	System.Net.Sockets	x	-	network	-	TypeRef	-	mscoree.dll
ProtocolType	System.Net.Sockets	x	-	network	-	TypeRef	-	mscoree.dll
Dns	System.Net	x	-	network	T1011 | Network Exfiltration	TypeRef	-	mscoree.dll
ICredentials	System.Net	x	-	network	T1011 | Network Exfiltration	TypeRef	-	mscoree.dll

Imagen 6. *Funciones importadas en el binario AsyncRAT: ColCERT.*

Durante el análisis de la muestra se identificó que el binario contiene la configuración completa del malware embebida de forma estática, una característica común en variantes de **AsyncRAT** utilizadas en campañas dirigidas. Esta configuración define parámetros críticos para la operación del implante, incluyendo la infraestructura de comando y control (C2), el puerto de comunicación y opciones relacionadas con la identificación y comportamiento del malware en el sistema comprometido.

El hallazgo de esta información embebida confirma que la muestra no depende de una descarga inicial de configuración externa para iniciar comunicaciones, lo que reduce la dependencia de infraestructura adicional y permite una activación inmediata tras la ejecución del binario. Este enfoque incrementa la efectividad de la infección inicial y dificulta su interrupción temprana mediante controles perimetrales.

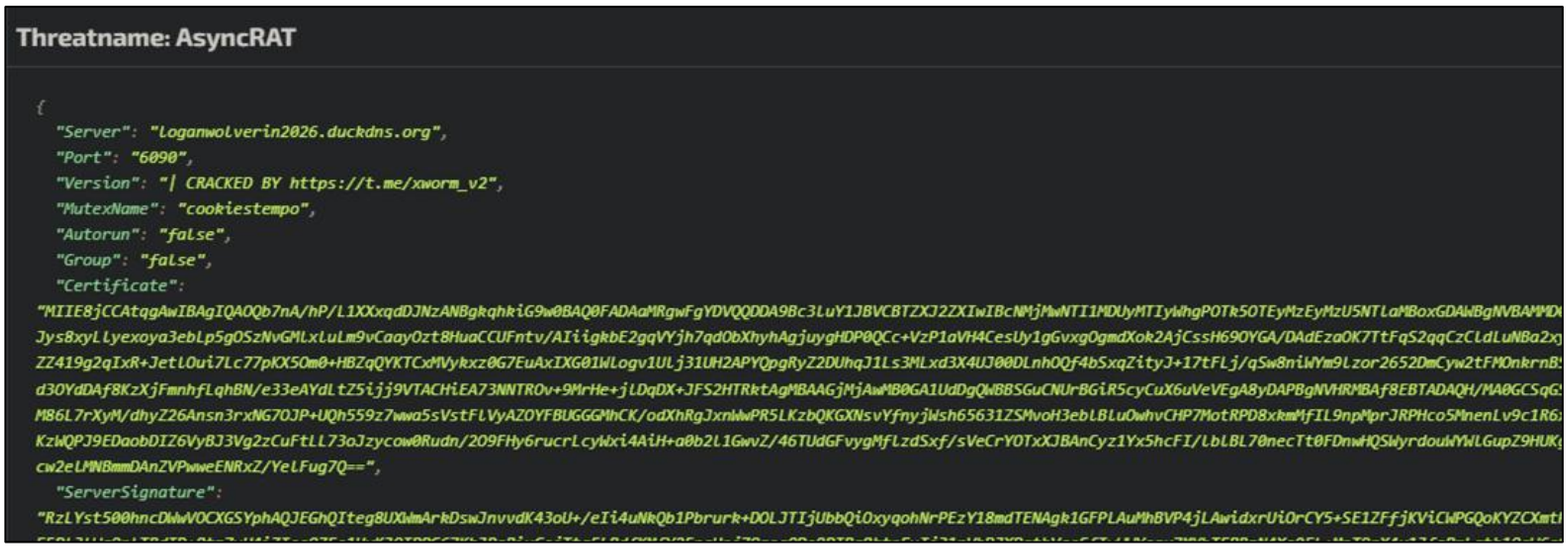

Imagen 7. *Configuración embebida en el binario AsyncRAT: ColCERT.*

Análisis dinámico

Se ejecutó la muestra en un entorno de pruebas controlado y se encontró que el binario presenta un comportamiento discreto y persistente desde su ejecución inicial. Durante el periodo de observación no se evidenció la creación de un árbol de procesos secundarios, ya que el ejecutable original se mantuvo activo y fue el encargado de gestionar directamente las distintas funcionalidades maliciosas.

La muestra realizó múltiples operaciones de lectura y consulta sobre claves asociadas a protocolos de red como **HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters**, lo que indica un interés en obtener información sobre la configuración de red del sistema comprometido. Este comportamiento es consistente con una fase de reconocimiento del entorno, en la que el *malware* recopila datos relacionados con interfaces de red, parámetros y posibles restricciones de conectividad. Esta información puede ser utilizada para adaptar la comunicación con la infraestructura de comando y control (C2), optimizar la estabilidad de las conexiones o detectar configuraciones atípicas asociadas a entornos de análisis.

12:29:...	AsyncRAT.exe	3848	RegCreateKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters
12:29:...	AsyncRAT.exe	3848	RegCreateKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters
12:29:...	AsyncRAT.exe	3848	RegSetInfoKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters
12:29:...	AsyncRAT.exe	3848	RegQueryKey	HKLM
12:29:...	AsyncRAT.exe	3848	RegQueryKey	HKLM
12:29:...	AsyncRAT.exe	3848	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Services\Dnscache\Parameters
12:29:...	AsyncRAT.exe	3848	RegOpenKey	HKLM\System\CurrentControlSet\Services\Dnscache\Parameters
12:29:...	AsyncRAT.exe	3848	RegSetInfoKey	HKLM\System\CurrentControlSet\Services\Dnscache\Parameters

Imagen 8. *Reconocimiento de parámetros de red de AsyncRAT: ColCERT.*

Asimismo, se observaron consultas y accesos a claves bajo **HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders,** las cuales permiten identificar rutas a directorios relevantes del perfil del usuario, como cachés, documentos o carpetas de uso frecuente. Este comportamiento sugiere que la muestra busca ubicar ubicaciones específicas del sistema de archivos que puedan ser utilizadas para almacenar archivos temporales, desplegar componentes adicionales o recolectar información sensible. El uso de rutas legítimas del perfil del usuario favorece la evasión, al mimetizar la actividad maliciosa con operaciones normales del sistema.

12:29:...	AsyncRAT.exe	3848	RegOpenKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
12:29:...	AsyncRAT.exe	3848	RegSetInfoKey	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
12:29:...	AsyncRAT.exe	3848	RegQueryValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Cache
12:29:...	AsyncRAT.exe	3848	RegCloseKey	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders

Imagen 9. *Consultas al registro sobre rutas relevantes: ColCERT.*

Finalmente, la muestra accedió a múltiples claves bajo **HKLM\SYSTEM\CurrentControlSet\Control\Session Manager**, incluyendo consultas a parámetros de control y políticas de recursos. Estas interacciones son indicativas de una verificación del estado del sistema y sus políticas de ejecución, potencialmente orientadas a asegurar la estabilidad del implante o evaluar condiciones que afecten su persistencia. En el contexto de **AsyncRAT**, este comportamiento puede asociarse a la preparación del entorno para una ejecución prolongada, así como a la identificación de restricciones que pudieran interferir con el funcionamiento continuo.

12:39:...	AsyncRAT.exe	3848	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager
12:39:...	AsyncRAT.exe	3848	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager
12:39:...	AsyncRAT.exe	3848	RegSetInfoKey	HKLM\System\CurrentControlSet\Control\Session Manager
12:39:...	AsyncRAT.exe	3848	RegQueryValue	HKLM\System\CurrentControlSet\Control\Session Manager\ResourcePolicies
12:39:...	AsyncRAT.exe	3848	RegCloseKey	HKLM\System\CurrentControlSet\Control\Session Manager

Imagen 10*. Consultas al registro sobre políticas: ColCERT.*

Conexiones

Durante el análisis dinámico se observó una consulta DNS exitosa hacia el dominio **loganwolverin2026[.]duckdns[.]org**, resuelta mediante el servidor público 8.8.8.8, obteniendo como respuesta una dirección IP pública asociada. Este comportamiento evidencia que la muestra utiliza un servicio de DNS dinámico (DuckDNS) como parte de su infraestructura de Comando y Control (C2).

314 27.953529	8.8.8.8	192.168.129.17	DNS	105 Standard query response 0x2997 A loganwolverin2026.duckdns.org A 192.169.69.26

Imagen 11. *Actividad DNS: ColCERT.*

El dominio **loganwolverin2026[.]duckdns[.]org** se encuentra asociado a un servicio de DNS dinámico, específicamente DuckDNS, y su infraestructura de red está vinculada al proveedor Stealthy Hosting, el cual ha sido históricamente relacionado con el alojamiento de infraestructura maliciosa. El uso de este tipo de servicios permite a los actores de amenaza rotar direcciones IP de forma ágil, manteniendo un punto de contacto estable para el malware sin necesidad de modificar la configuración embebida en las muestras distribuidas.

Desde el punto de vista de reputación, el dominio se encuentra clasificado como no confiable (Untrusted) y categorizado dentro de sitios maliciosos, con registro activo en listas de bloqueo de inteligencia de amenazas. En particular, ha sido incluido en listas de bloqueo, con una clasificación explícita como malicioso, lo que confirma su uso en actividades asociadas a *malware* y comando y control. La fecha de primera detección indica que esta infraestructura ha estado activa desde finales de 2025, manteniéndose operativa durante el periodo analizado.

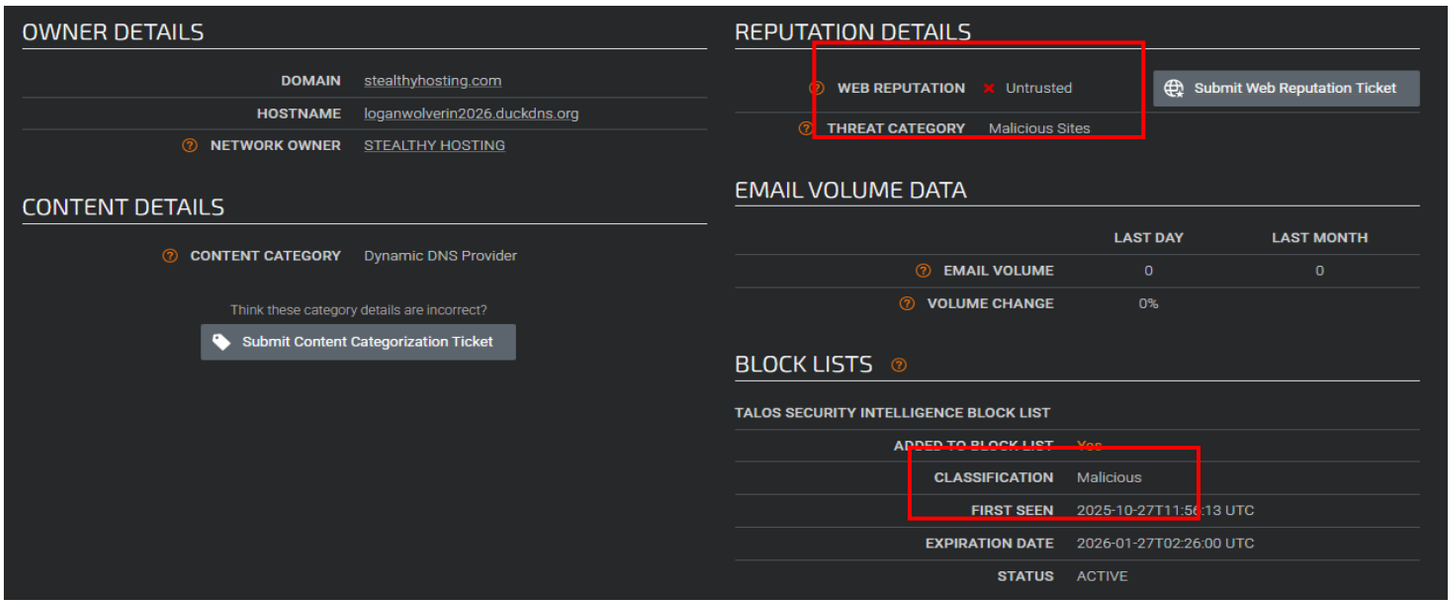

Imagen 12. *Reputación del dominio: ColCERT.*

Posteriormente, se observó actividad de red constante generada por el proceso **AsyncRAT.exe**, la cual consistió en múltiples intentos de conexión TCP hacia un dominio remoto utilizando el puerto 6090, valor que se encontraba definido de forma explícita en la configuración embebida del malware, tal como se evidenció durante el análisis estático de la muestra.

La insistencia en reconectar y el uso de un puerto no estándar refuerzan la atribución de esta actividad a un implante de acceso remoto plenamente funcional, alineado con el modus operandi de **APT-C-36**. Este comportamiento constituye un indicador claro de intento de comunicación C2 y resulta clave para la detección temprana en entornos de red institucionales.

12:40:...	AsyncRAT.exe	3848	TCP Connect	DESKTOP-E2R55TU:14456 -> sinkhole.hyas.com:6090
12:40:...	AsyncRAT.exe	3848	TCP Receive	DESKTOP-E2R55TU:14456 -> sinkhole.hyas.com:6090
12:40:...	AsyncRAT.exe	3848	TCP Disconnect	DESKTOP-E2R55TU:14456 -> sinkhole.hyas.com:6090
12:40:...	AsyncRAT.exe	3848	TCP Connect	DESKTOP-E2R55TU:14460 -> sinkhole.hyas.com:6090
12:40:...	AsyncRAT.exe	3848	TCP Receive	DESKTOP-E2R55TU:14460 -> sinkhole.hyas.com:6090
12:40:...	AsyncRAT.exe	3848	TCP Disconnect	DESKTOP-E2R55TU:14460 -> sinkhole.hyas.com:6090
12:40:...	AsyncRAT.exe	3848	TCP Connect	DESKTOP-E2R55TU:14461 -> sinkhole.hyas.com:6090
12:40:...	AsyncRAT.exe	3848	TCP Receive	DESKTOP-E2R55TU:14461 -> sinkhole.hyas.com:6090
12:40:...	AsyncRAT.exe	3848	TCP Disconnect	DESKTOP-E2R55TU:14461 -> sinkhole.hyas.com:6090
12:40:...	AsyncRAT.exe	3848	TCP Connect	DESKTOP-E2R55TU:14463 -> sinkhole.hyas.com:6090
12:40:...	AsyncRAT.exe	3848	TCP Receive	DESKTOP-E2R55TU:14463 -> sinkhole.hyas.com:6090

Imagen 13. *Actividad TCP: ColCERT.*

Técnicas MITRE ATT&CK

Táctica	ID Técnica	Nombre de la Técnica	Uso específico por APT-C-36 (Blind Eagle)
Reconnaissance	T1598.003	Phishing for information / Spearphishing Link	Crean correos que parecen notificaciones reales de la DIAN, la Fiscalía o la Rama Judicial. El enlace direcciona Google Drive o MediaFire donde tienen alojado el virus disfrazado de "Citación" o "Multa"
Resource Development	T1588.001	Obtain Capabilities: Malware	Usan troyanos gratuitos (AsyncRAT) para no dejar huellas de código propio.
Initial Access	T1566.001	Phishing: Spearphishing Attachment	Envío de correos suplantando a la DIAN o Fiscalía con archivos HTML/SVG
	T1566.002	Spearphishing Link	Envío de correos suplantando a la DIAN o Fiscalía con links a Google Drive
Execution	T1204.001	User Execution: Malicious Link	Dependencia crítica de que el usuario haga clic en el enlace
	T1204.002	User Execution: Malicious File	Dependencia crítica de que el usuario ejecute el archivo comprimido
	T1059.001	Command and Scripting Interpreter: PowerShell	Uso intensivo de PowerShell para descargar el payload final (AsyncRAT)
	T1059.005	Command and Scripting Interpreter: Visual Basic	Uso intensivo de VBScript para descargar el payload final (AsyncRAT)
	T1047	Windows Management Instrumentation (WMI)	Aunque no se detalla un comando específico, el uso de herramientas RAT como AsyncRAT suele implicar consultas WMI para perfilado, alineado con la recolección de datos del sistema descrita
Persistence	T1547.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	Modificación del registro de Windows para ejecutarse automáticamente al iniciar sesión
	T1053.005	Scheduled Task/Job: Scheduled Task	Creación de tareas automáticas para asegurar la ejecución persistente en el tiempo
Defense Evasion	T1036.004	Masquerading: Masquerade Task or Service	Uso de iconos de PDF para ejecutables y nombres de archivos que imitan documentos legales
	T1027	Obfuscated Files or Information	Uso de empacadores (packers) y código "enredado" para que los antivirus no reconozcan el RAT
	T1574.002	Hijack Execution Flow: DLL	El malware AsyncRAT analizado fue compilado en VB.NET, lo que facilita la ofuscación y carga dinámica de componentes para evadir firmas estáticas
	T1140	Deobfuscate/Decode Files or Information	El malware se "arma" a sí mismo en memoria tras la descarga para evitar escaneos de disco
Discovery	T1012	Query Registry	Hace múltiples consultas al registro para verificar políticas de control y estado del sistema
	T1083	File and Directory Discovery	Escaneo de carpetas del sistema y llaves de registro para perfilar a la víctima y buscar archivos clave
	T1016	System Network Configuration Discovery	El malware consulta claves de registro para entender la configuración de red de la víctima
Collection	T1056.001	Input Capture: Keylogging	Registro de todas las pulsaciones de teclado para robar credenciales bancarias y correos
	T1113	Screen Capture	La funcionalidad de AsyncRAT y las importaciones de API gráfica sugieren capacidad de vigilancia y monitoreo visual
Command and Control	T1568.002	Dynamic Resolution: Domain Generation Algorithms	Uso de DuckDNS (ej. loganwolverin2026[.]duckdns[.]org) para cambiar IPs rápidamente
	T1571	Non-Standard Port	Comunicación a través del puerto 6090 para evadir filtros de navegación web básica
	T1001.002	Data Obfuscation / Steganography	El grupo ha comenzado a usar imágenes (a veces fotos de documentos o logotipos institucionales) que contienen dentro el código de sus RATs (como AsyncRAT)
	T1105	Ingress Tool Transfer	Uso de funciones como WebClient y DownloadFile para descargar módulos adicionales o actualizaciones desde internet
	T1071.001	Web Protocols	Uso de tráfico web para la comunicación inicial y descarga de payloads desde servicios de nube legítimos

Tabla 2. *TTP de* ***APT-C-36****: ColCERT.*

Técnicas MITRE ATT&CK

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Defense Evasion	Discovery	Collection	Command and Control
T1598.003 Phishing for information: Spearphishing Link	T1588.001 Obtain Capabilities: Malware	T1566.001 Phishing: Spearphishing Attachment	T1204.001 User Execution: Malicious Link	T1547.001 Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	T1036.004 Masquerading: Masquerade Task or Service	T1012 Query Registry	T1056.001 Input Capture: Keylogging	T1568.002 Dynamic Resolution: Domain Generation Algorithms
		T1566.002 Phishing: Spearphishing Link	T1204.002 User Execution: Malicious File	T1053.005 Scheduled Task/Job: Scheduled Task	T1027 Obfuscated Files or Information	T1083 File and Directory Discovery	T1113 Screen Capture	T1571 Non-Standard Port
			T1059.001 Command and Scripting Interpreter: PowerShell		T1574.002 Hijack Execution Flow: DLL	T1016 System Network Configuration Discovery		T1001.002 Data Obfuscation / Steganography
			T1059.005 Command and Scripting Interpreter: Visual Basic		T1140 Deobfuscate/Decode Files or Information			T1105 Ingress Tool Transfer
			T1047 Windows Management Instrumentation (WMI)					T1071.001 Web Protocols

Imagen 14. *Matriz ATT&CK de* ***APT-C-36****: ColCERT.*

Indicadores de compromiso IoCs

Archivos:

- **MD5**: 885127590b2c7ec029e1c5aab5d0635a
- **SHA1**: a74100abab8962b0cdc97bedb9399180443c0f3e
- **SHA256**: 8e1f62b87234e54baf7ca40bfd2a81a6ed53b5a009b15ce7e4cba7d54d39a3a2

DNS:

- loganwolverin2026[.]duckdns[.]org

IP:

- 192 [.] 169 [.] 69 [.] 26

Conclusiones

El análisis consolidado de la actividad asociada a **APT-C-36** (Blind Eagle / TAG-144) confirma que se trata de un actor de amenazas persistente, activo y altamente especializado en el contexto colombiano, con un enfoque sostenido en campañas de *phishing* dirigido contra entidades gubernamentales y sectores estratégicos. Su conocimiento del entorno administrativo, legal y burocrático del país le permite diseñar señuelos convincentes que incrementan significativamente la probabilidad de compromiso exitoso.

El análisis estático y dinámico de la muestra examinada demuestra un comportamiento coherente con campañas previamente atribuidas al grupo, incluyendo comunicación cifrada con infraestructura C2, reconexiones persistentes, uso de puertos no estándar y mecanismos de evasión frente a entornos de análisis. La correlación entre los parámetros embebidos en el binario y la actividad de red observada valida la atribución técnica y confirma la capacidad del actor para mantener control prolongado sobre sistemas comprometidos.

En conjunto, **APT-C-36** representa una amenaza relevante y continua para el ecosistema digital colombiano, especialmente para entidades públicas con alta exposición al correo electrónico y procesos administrativos digitalizados. Su enfoque regional, persistencia operativa y adaptación constante subrayan la necesidad de reforzar las capacidades de detección temprana, concienciación del personal y monitoreo de infraestructura de red, así como de mantener una vigilancia activa sobre este actor y sus campañas emergentes.

Para fortalecer la postura de defensa frente a las campañas atribuidas a **APT-C-36** y reducir el riesgo de compromiso mediante herramientas de acceso remoto como **AsyncRAT**, se recomienda:

- ❑ Aislar de manera inmediata los equipos que presenten indicios de infección y bloquear dominios e IPs asociados a infraestructura de comando y control (C2) identificada, incluyendo servicios de DNS dinámico, mediante reglas en firewall, proxy y soluciones de filtrado DNS.
- ❑ Implementar monitoreo del tráfico saliente para detectar conexiones persistentes o reconexiones frecuentes hacia dominios poco comunes, servicios de DNS dinámico y puertos no estándar, especialmente aquellos definidos estáticamente en configuraciones de *malware*.
- ❑ Fortalecer los controles de seguridad en correo electrónico, priorizando la detección y bloqueo de archivos URL, HTML, SVG y enlaces embebidos que redirijan a recursos externos, así como la inspección de mensajes que suplantan entidades estatales o administrativas.
- ❑ Realizar campañas de concientización dirigidas a funcionarios y personal administrativo, enfocadas en la detección de correos de phishing que suplantan entidades como la DIAN, Rama Judicial o Fiscalía, enfatizando la verificación del remitente, enlaces y urgencia artificial en las comunicaciones.

Resumen de las fuentes y nivel de confianza en la información proporcionada

El presente informe se fundamenta en un conjunto de fuentes especializadas de alta credibilidad que permiten sostener con solidez los hallazgos y conclusiones. Con base en la estabilidad y reputación de estas fuentes, el nivel de confianza general de la información analizada se clasifica como alto, aunque se reconocen limitaciones inherentes, como la ausencia de telemetría regional completa y posibles vacíos sobre actividades emergentes que aún no cuentan con documentación abierta suficiente.

Recorded Future, 26 de agosto de 2025, "TAG-144's Persistent Grip on South American Organizations, Informe de proveedor de ciberseguridad.
https://assets.recordedfuture.com/insikt-report-pdfs/2025/cta-2025-0826.pdf.
The Hacker News, 27 de agosto de 2025, "Blind Eagle's Five Clusters Target Colombia Using RATs, Phising Lures, and Dynamic DNS", Medio especializado en noticias de ciberseguridad.
https://thehackernews.com/2025/08/blind-eagles-five-clusters-target.html.
Ingeniería Telemática, 27 de agosto de 2025, "Blind Eagle: Campañas de Ciberespionaje Dirigidas a Colombia con RATs y Phishing", Portal de proveedor de ciberseguridad.
https://www.ingenieriatelematica.com.co/blind-eagle-campanas-ciberespionaje-Colombia.
Fuentes internas ColCERT.