Alerta

Actividad de Remcos RAT vinculada a APT-C-36

COLCERT AL – 20260801 - 104

TIC

TLP:CLEAR

Resumen Ejecutivo

Los análisis forense ha confirmado la infección con Remcos RAT, un troyano comercial frecuentemente empleado por actores de amenaza como Blind Eagle (APT-C-36 / TAG-144), un grupo históricamente enfocado en organizaciones Latinoamericanas. El vector de compromiso inicial empleó phishing con un señuelo de "pago a proveedores", distribuyendo archivos VBS que iniciaron una cadena de ejecución multietapa (VBS → BAT → EXE → VBS → JS), la cual culminó con la inyección del payload final (svchot.exe), diseñado para enmascararse como un proceso legítimo del sistema.

Para asegurar la persistencia, el atacante configuró una tarea programada camuflada como un servicio de OneDrive y abusó de BITS (bitsadmin) para realizar descargas encubiertas, simulando actualizaciones de Microsoft Defender. Finalmente, la operación se soporta sobre una infraestructura de comando y control (C2) de tres niveles (staging → relay → C2 Remcos) basada en DuckDNS, la cual canaliza el tráfico hacia un proveedor de alojamiento en Rumania (AS9009 / M247).

NIVEL DE RIESGO

ALTO

Impacto técnico confirmado por las capacidades de Remcos RAT

- ❑ Acceso remoto completo e interactivo al host comprometido.
- ❑ Extracción de credenciales almacenadas en navegadores/clientes de correo y aplicaciones locales
- ❑ Registro de pulsaciones de teclado - Keylogging
- ❑ Capturas de pantalla, así como intercepción de periféricos de audio y video (webcam/micrófono).
- ❑ Exfiltración de archivos y documentos sensibles.
- ❑ Ejecución remota de comandos, scripts y despliegue de binarios maliciosos adicionales.

Contexto de la amenaza

Perfil del actor: Blind Eagle (también identificado como APT-C-36, TAG-144, AguilaCiega y APT-Q-98) es un actor de Amenaza Persistente Avanzada (APT) con actividad documentada desde 2018. Su operación se concentra casi exclusivamente en organizaciones e individuos de habla hispana, consolidándose como uno de los grupos con mayor continuidad operativa y volumen de ataques dirigidos contra Colombia, con incursiones adicionales registradas en Ecuador, Chile y Panamá.

A diferencia de adversarios globales que reciclan campañas de phishing mediante traducciones genéricas, Blind Eagle demuestra un profundo entendimiento del entorno normativo, administrativo e institucional colombiano. Esta inteligencia regional le permite diseñar campañas de ingeniería social altamente contextualizadas, utilizando señuelos que suplantan con gran precisión las comunicaciones oficiales, lo que incrementa drásticamente su tasa de éxito en la fase de acceso inicial.

Motivación: La actividad de Blind Eagle responde principalmente a objetivos de ciberespionaje, sustracción de credenciales, acceso persistente y recolección de información confidencial. Las campañas atribuidas al grupo buscan garantizar una presencia prolongada en los entornos vulnerados para ejecutar labores de vigilancia continua y exfiltrar datos estratégicos. Posteriormente, estos activos pueden ser monetizados o empleados para facilitar el escalamiento de privilegios y el movimiento lateral hacia otros segmentos de la infraestructura afectada.

Mapeo Táctico MITRE ATT&CK

A continuación, se presenta la tabla detallada de las Tácticas, Técnicas y Procedimientos (TTPs) identificadas, mapeadas con el marco de MITRE ATT&CK.

Táctica	ID Técnica	Descripción Técnica Observada
Reconocimiento	**T1583.001 Adquisición de Infraestructura: Dominios**	Registro y utilización de múltiples subdominios de DuckDNS para funciones de staging, retransmisión (relay) y comando y control (C2).
	T1584.005 Compromiso de Infraestructura: Botnet / Alojamiento	Uso de infraestructura alojada sobre el AS9009 (M247, Rumania), proveedor de alojamiento frecuentemente asociado con actividades maliciosas.
Acceso Inicial	**T1566.001 Phishing: Archivo Adjunto de Spearphishing**	Distribución de los archivos PAGO PROVEEDOR.vbs y Soporte de pago.vbs mediante correos electrónicos con temática de pagos a proveedores para inducir su ejecución.
Ejecución	**T1204.002 Ejecución por el Usuario: Archivo Malicioso**	El usuario ejecuta manualmente el archivo VBS adjunto, iniciando la cadena de infección.
	T1059.005 Intérprete de Comandos y Scripts: Visual Basic	Ejecución de múltiples scripts VBS (avg.vbs, dmw.vbs, PAGO PROVEEDOR.vbs y Soporte de pago.vbs) mediante wscript.exe.
	T1059.003 Intérprete de Comandos y Scripts: Símbolo del Sistema de Windows	Los archivos star.bat y dmw.bat implementan la lógica de orquestación, descarga de componentes y limpieza del sistema.
	T1059.007 Intérprete de Comandos y Scripts: JavaScript	Ejecución del script dmw.js como etapa final del cargador (loader) antes de iniciar la carga útil (payload).
Persistencia	**T1053.005 Tareas Programadas: Tarea Programada**	Creación de la tarea programada OneDrive Startup Task-S-1-5-..., configurada para ejecutar avg.vbs en cada inicio de sesión del usuario.
	T1197 Trabajos BITS	Creación y reutilización del trabajo BITS Update_Windows_Defender para mantener la persistencia y descargar componentes adicionales.
Evasión de Defensas	**T1036.005 Enmascaramiento: Coincidencia con un Nombre Legítimo**	Uso de nombres similares a componentes legítimos del sistema, como OneDrive Startup Task, svchot.exe y Update_Windows_Defender, para reducir la probabilidad de detección.
	T1027 Archivos o Información Ofuscados	Empleo de scripts VBS ofuscados durante toda la cadena de infección para dificultar el análisis y la detección.
	T1070.004 Eliminación de Indicadores: Borrado de Archivos	Eliminación de archivos temporales mediante star.bat con el fin de reducir evidencias forenses.
	T1574 Secuestro del Flujo de Ejecución (Búsqueda de DLL)	Presencia de winmm.dll junto al payload en C:\windll\, consistente con una técnica de secuestro del orden de búsqueda de bibliotecas DLL.
	T1218 (Inferida) Ejecución Mediante Binarios Legítimos del Sistema	Uso de binarios legítimos de Windows, como wscript.exe y bitsadmin, para ejecutar código malicioso y evadir controles de seguridad.
Comando y Control	**T1071.001 Protocolo de Capa de Aplicación: Protocolos Web**	Comunicación mediante HTTP con restoredataserver.duckdns[.]org:8060 para la descarga de componentes y el establecimiento del canal C2.
	T1105 Transferencia de Herramientas hacia el Sistema Comprometido	Descarga de múltiples componentes (dmw.js, svchot.exe) desde el servidor de staging utilizando el servicio BITS.
	T1090 Proxy	El dominio conectiondriverswin.duckdns[.]org (128.90.115.210) actúa como nodo intermediario (relay) entre la víctima y el servidor de comando y control.
	T1568.002 Resolución Dinámica	Uso intensivo de DuckDNS para la resolución dinámica de dominios, dificultando la implementación de bloqueos basados en indicadores estáticos.
	T1219 Software de Acceso Remoto	Utilización de Remcos RAT como herramienta de acceso remoto para el control de los sistemas comprometidos.

Táctica	ID Técnica	Descripción Técnica Observada
Recolección / Acceso a Credenciales / Exfiltración (Inferida)	**T1056.001 Captura de Entrada: Registro de Pulsaciones (Keylogging)**	Capacidad nativa de Remcos RAT para registrar las pulsaciones del teclado de la víctima.
	T1113 Captura de Pantalla	Funcionalidad integrada para capturar imágenes de la pantalla del sistema comprometido.
	T1005 Obtención de Datos del Sistema Local	Recolección de archivos y documentos almacenados en el equipo comprometido para su posterior exfiltración.
	T1555 Obtención de Credenciales desde Almacenes de Contraseñas	Capacidad para extraer credenciales almacenadas en navegadores web y clientes de correo compatibles.
	T1041 Exfiltración a Través del Canal de Comando y Control	Transferencia de la información recopilada utilizando el mismo canal de comunicaciones empleado para el comando y control.

Cadena de Ataque (Kill Chain)

La cadena de ataque describe la secuencia de actividades empleadas por el actor de amenazas, desde la entrega del malware mediante phishing hasta el establecimiento del canal de comando y control y la ejecución del payload final.

Indicadores de Compromiso (IOCs)

Dominios e infraestructura

Indicador	Rol	Detalle
restoredataserver.duckdns[.]org:8060	Servidor de staging	Descarga, staging, payloads y scripts. Entrega svchot.exe.
conectiondriverswin.duckdns[.]org	Relay / puente	Resuelve a 128.90.115.210:8060.
128.90.115.210	IP del nodo relay	AS9009 (M247), Rumania.
reconexionservidor.duckdns[.]org	Servidor C2 (Remcos)	Confianza ThreatFox: 100%. Hosting AS9009 M247, Rumania.

Categoría	Indicador de Compromiso (IoC)	Descripción
URL	http://restoredataserver.duckdns[.]org:8060/data/Descargas/dmw.js	URL utilizada para la descarga del script dmw.js desde el servidor de staging. Se recomienda verificar la ruta exacta en los registros originales antes de utilizarla en reglas de detección.
Archivo	C:\win\avg.vbs	Script VBS utilizado para mantener la persistencia mediante tarea programada.
Archivo	C:\win\star.bat	Script por lotes encargado de la orquestación, limpieza de artefactos y evasión de detección.
Archivo	C:\win\dmw.exe	Componente intermedio de la cadena de infección.
Archivo	C:\win\dmw.bat	Script de apoyo para la ejecución del cargador (loader).
Archivo	C:\win\dmw.vbs	Script VBS utilizado durante las etapas intermedias de ejecución.
Archivo	C:\win\dmw.js	Script JavaScript descargado desde la infraestructura del atacante antes de ejecutar el payload final.
Archivo	C:\win\Quiet.exe	Ejecutable auxiliar empleado durante la cadena de ejecución.
Archivo	C:\win\BIT*.tmp	Archivos temporales generados por transferencias BITS, correspondientes a descargas fallidas o incompletas.
Archivo	C:\windll\svchot.exe	Payload final de Remcos RAT, cuyo nombre suplanta al proceso legítimo svchost.exe.
Archivo	C:\windll\PAGO PROVEEDOR.vbs	Dropper inicial distribuido mediante campaña de phishing.
Archivo	C:\windll\Soporte de pago.vbs	Variante del dropper inicial utilizada en la campaña maliciosa.
Archivo	C:\windll\winmm.dll	Biblioteca DLL posiblemente utilizada para implementar un ataque de DLL Search Order Hijacking.
Persistencia	OneDrive Startup Task-S-1-5-21-2448532352-3014186884-3468110516-1001	Tarea programada creada para ejecutar avg.vbs en cada inicio de sesión y mantener la persistencia.
Persistencia	Update_Windows_Defender	Trabajo BITS utilizado para descargar componentes adicionales y mantener la persistencia del malware.

Hashes de Archivos (SHA-256)

Archivo	SHA-256
svchot.exe	7E7A25F4461A3A3AAFAC3EED7E732F0BD5612FDE6FB8163F8AC3DC781C3E5396
Quiet.exe	C22904610319843578ADA35FB483D219BD007DA69179D57C7E1223CAB078492C
PAGO PROVEEDOR.vbs	17CFD817D086D586AF8FE7AD961AFCCD8AC44BA28BEFB263228B1A282177D55
Soporte de pago.vbs	BB13A2F5A1A360BF5528BA2039BEC21EA6AB27F22848222049C14E03C01E6AB9
dmw.vbs	40597DC6B5E20B052C57F118A1E2E378007EDE38CEEFCCE751D7AF831DAAA068
avg.vbs	45AE6709E1ACFDAA9C67990154741A454CC4596A9BF2C50644416652017FCCB2
star.bat	DABCBB20F3CB396E53F63C2BDA29E191377C48145A0B39387CAAEC06EB37E34

Recomendaciones de defensa

Con base en los hallazgos obtenidos durante el análisis, se recomienda implementar las siguientes medidas para fortalecer las capacidades de prevención, detección, contención y respuesta frente a campañas que empleen técnicas similares a las observadas.

Contención y erradicación

- ❑ Aislar de la red los equipos en los que se identifiquen indicadores de compromiso asociados con la campaña, con el fin de evitar la propagación del incidente y preservar la evidencia digital.
- ❑ Eliminar los mecanismos de persistencia utilizados por el malware, incluyendo tareas programadas, trabajos BITS y cualquier otro artefacto que permita la ejecución automática de los componentes maliciosos.
- ❑ Preservar los archivos y artefactos identificados en un entorno seguro antes de su eliminación, permitiendo su análisis forense, la generación de nuevos indicadores de compromiso y la correlación con investigaciones posteriores.

Protección de la infraestructura

- ❑ Incorporar los indicadores de compromiso identificados en los equipos de bloqueo y monitoreo, firewalls, servicios DNS, proxies y plataformas IDS/IPS.
- ❑ Implementar controles que permitan detectar y restringir conexiones salientes hacia infraestructuras no autorizadas, especialmente aquellas que utilicen protocolos web y puertos no estándar para establecer canales de comando y control (C2).
- ❑ Restringir la resolución de dominios de DNS dinámico cuando no exista una necesidad operativa justificada, reduciendo el riesgo asociado con infraestructuras utilizadas por actores de amenazas.
- ❑ Realizar la rotación periódica de credenciales de todos los usuarios, incluyendo cuentas de dominio, correo electrónico, VPN y aplicaciones críticas del negocio.

Endurecimiento de los equipos

- ❑ Restringir la ejecución de intérpretes de scripts como wscript.exe y cscript.exe, así como de herramientas administrativas susceptibles de ser utilizadas como Living-off-the-Land Binaries (LOLBins), entre ellas bitsadmin.exe, mediante mecanismos como AppLocker, Windows Defender Application Control (WDAC) o soluciones equivalentes.
- ❑ Bloquear o poner en cuarentena archivos adjuntos ejecutables o de scripting, particularmente aquellos con extensiones .vbs, .js, .bat y .hta, salvo que exista una necesidad operacional debidamente justificada.
- ❑ Implementar controles de integridad que permitan detectar modificaciones no autorizadas en bibliotecas DLL y reducir el riesgo de técnicas como DLL Search Order Hijacking.

Concienciación y capacitación

- ❑ Desarrollar campañas de sensibilización dirigidas a usuarios con funciones administrativas, financieras y contables, enfocadas en la identificación de intentos de phishing relacionados con pagos a proveedores, facturación y otras temáticas frecuentemente utilizadas por este tipo de actores.
- ❑ Reforzar las buenas prácticas de manejo de archivos adjuntos y la verificación de la legitimidad de comunicaciones provenientes de entidades externas.

Fuentes

COLCERT. (2026, 5 de febrero). Seguimiento a la actividad del actor APT-C-36 (Informe COLCERT IN-20260209-028, TLP:CLEAR).
https://www.colcert.gov.co/800/w3-article-427530.html

Recorded Future, Insikt Group. (2025, 26 de agosto). TAG-144's persistent grip on South American organizations.
https://assets.recordedfuture.com/insikt-report-pdfs/2025/cta-2025-0826.pdf

The Hacker News. (2025, 27 de agosto). Blind Eagle's five clusters target Colombia using RATs, phishing lures, and dynamic DNS infra.
https://thehackernews.com/2025/08/blind-eagles-five-clusters-target.html

Ingeniería Telemática S.A.S. (2025, 27 de agosto). Blind Eagle: Campañas de ciberespionaje dirigidas a Colombia con RATs y phishing.
https://www.ingenieriatelematica.com.co/blind-eagle-campanas-ciberespionaje-colombia/

The MITRE Corporation. (s. f.). MITRE ATT&CK®: Knowledge base of adversary tactics and techniques.
https://attack.mitre.org/