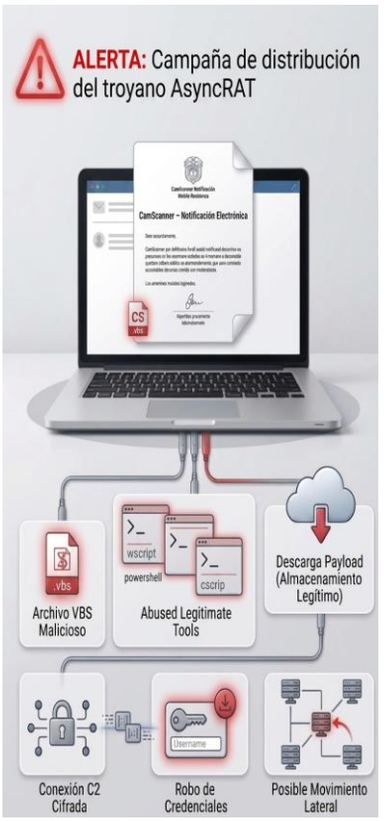
Alerta

Campaña de distribución del troyano AsyncRAT

COLCERT AL – 20260818 - 112

TLP:CLEAR

Resumen Ejecutivo



Se identificó una campaña activa de distribución del troyano de acceso remoto AsyncRAT, **dirigida a organizaciones en Colombia con impacto potencial en los sectores de Gobierno, Financiero, Servicios Corporativos y Retail.** La cadena de infección inicia mediante técnicas de ingeniería social que suplantan notificaciones electrónicas judiciales u oficiales y aparentan contener documentos escaneados mediante la aplicación CamScanner, distribuidos en archivos con extensión .vbs (Visual Basic Script).

La amenaza emplea técnicas de enmascaramiento de archivos (Masquerading) y abusa de binarios legítimos del sistema operativo (LOLBins) como wscript.exe, cscript.exe, PowerShell.exe y MSBuild.exe para evadir controles perimetrales y de endpoint. El payload principal es descargado desde repositorios legítimos en Google Firebase Storage, reduciendo la efectividad de los bloqueos basados únicamente en reputación de dominio. *Una vez desplegado, el malware establece comunicación con infraestructura de Comando y Control (C2) cifrada mediante AES sobre un subdominio de DNS dinámico (DuckDNS) y ejecuta intentos de inyección de memoria sobre el proceso lsass.exe con fines de robo y escalamiento de credenciales locales/de dominio.*

Como resultado del análisis, se identificaron 32 muestras de archivos mediante sus hashes SHA-256, un dominio de C2,-- DuckDNS, una URL de descarga del payload en Google Firebase Storage y 9 direcciones IP relacionadas con la infraestructura de red del atacante. Debido a sus capacidades de espionaje, robo de credenciales en memoria, persistencia y facilitación de movimiento lateral o despliegue de amenazas secundarias en redes corporativas, **esta campaña se categoriza con un nivel de severidad ALTO.**

Introducción

La actividad fue identificada en Colombia y corresponde a una muestra maliciosa en formato VBScript, distribuida mediante un esquema de ingeniería social que suplanta la identidad visual y la nomenclatura de la aplicación de digitalización de documentos CamScanner, el archivo incorpora además referencias a supuestas “notificaciones electrónicas judiciales/oficiales”, para generar confianza, aparentar ser un documento legítimo (como un PDF) e inducir a la víctima a su ejecución.

La amenaza presenta un alcance intersectorial, con potencial de afectación a organizaciones de los sectores Gobierno, Financiero, Servicios Corporativos y Retail, su impacto se incrementa por el uso de servicios cloud legítimos para la evasión de controles perimetrales y por la incorporación de capacidades orientadas a la extracción de credenciales, incluyendo intentos de inyección sobre el proceso lsass.exe. Estas acciones facilitan el compromiso de cuentas privilegiadas y el posterior movimiento lateral dentro de las redes corporativas.

Adicionalmente, el builder (constructor) utilizado presenta la leyenda “CRACKED BY”, acompañada de una referencia al canal de Telegram t.me/xworm_v2. Este indicador sugiere el uso de una versión modificada o crackeada de un generador asociado a malware de tipo commodity, cuya distribución y/o promoción estaría vinculada a dicho canal.

Técnicas y Tácticas — MITRE ATT&CK

A continuación se detalla el ciclo de ataque documentado, organizado por fases.

Táctica	ID de técnica	Procedimiento
Acceso Inicial	T1566.001	Spearphishing Attachment: adjunto malicioso .vbs entregado simulando ser un documento escaneado (CamScanner).
Ejecución	T1059.005	Visual Basic: uso de VBScript como cargador inicial, procesado por wscript.exe.
Ejecución	T1059.001	PowerShell: ejecución de scripts con omisión de las directivas de ejecución mediante -ExecutionPolicy Bypass.
Evasión de Defensas	T1036.005	Coincidencia con nombre o ubicación legítimos: mascarada del archivo imitando una digitalización de CamScanner.
Evasión de Defensas	T1027	Archivos o información ofuscados: uso de Base64 y scripts ofuscados descargados desde Firebase.
Evasión de Defensas	T1055.001	Inyección de DLL: inyección de binarios maliciosos mediante MSBuild.exe e intentos de inyección en lsass.exe.
Acceso a Credenciales	T1003.001	Memoria de LSASS: intento de acceso a la memoria de lsass.exe para el volcado de credenciales corporativas.
Comando y Control	T1071.001	Protocolos web: descarga de artefactos vía HTTPS utilizando la infraestructura de Google Firebase Storage.
Comando y Control	T1568.002	DNS dinámico: infraestructura de C2 vinculada a un proveedor de DNS dinámico (duckdns.org).
Comando y Control	T1573.001	Criptografía simétrica: comunicación C2 con payload cifrado mediante una clave AES.

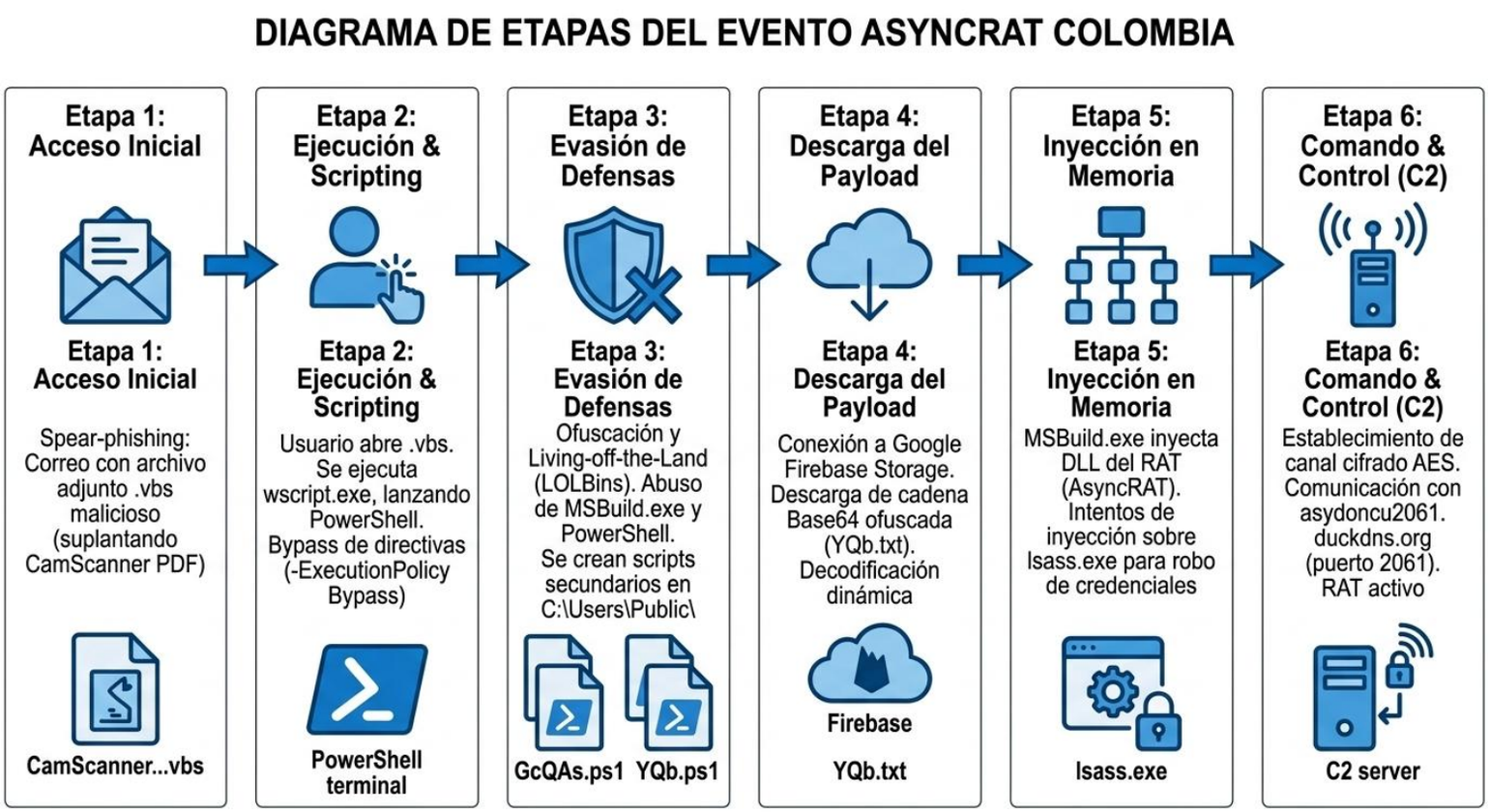
Cadena de infección y comportamiento técnico

- **Ejecución y Bypass de Políticas (LOLBins):** El script .vbs inicial ejecuta comandos en PowerShell forzando la omisión de restricciones de ejecución (-ExecutionPolicy Bypass), creando y desplegando scripts secundarios (GcQAs.ps1 y YQb.ps1) en el directorio público C:\Users\Public\.

- **Descarga de Payload Secundario (Cloud Staging):** Conecta a una instancia en Google Firebase [hxxps://firebasestorage[.]googleapis[.]com/.../dll.txt] para recuperar una cadena cifrada/ofuscada (YQb.txt), la cual es procesada y decodificada dinámicamente en memoria con Base64.

- **Inyección en Procesos y Compromiso de LSASS:** El script invoca el compilador legítimo de Microsoft .NET (MSBuild.exe) para realizar Process Injection de la DLL cargadora. Durante los análisis dinámicos, se registraron intentos directos de inyectar librerías no firmadas (EwLruCKL.dll) dentro del proceso del sistema lsass.exe, con el objetivo de realizar volcado de memoria y extracción de credenciales administrativas.

- **Comando y Control (C2) y Persistencia:** La etapa final despliega AsyncRAT, instalándose en %AppData%, creando un mutex de instancia única (AsyncMutex_6SI8OkPnk) y estableciendo comunicaciones cifradas mediante AES con la infraestructura C2 hospedada en DNS dinámico (asydoncu2061.duckdns.org en el puerto TCP 2061).



Indicadores de Compromiso (IoCs)

Infraestructura de red — Dominios y URL

Tipo	Indicador / Dominio	Descripción
C2	asydoncu2061.duckdns.org	Servidor de Comando y Control (C2), puerto TCP 2061
Hosting del payload	firebasestorage.googleapis.com	Infraestructura utilizada para alojar/descargar el payload
URL de descarga	hxxps://firebasestorage[.]googleapis[.]com/v0/b/rodriakd-8413d.appspot[.]com/o/dll/dll.txt?alt=media&token=64749d51-8c6f-484b-b0f1-f9ebba5ae15e	URL específica utilizada para la descarga del archivo dll.txt desde Firebase Storage

Muestras de Archivos y Hashes (SHA256)

- 2a77e7e02974ff951fe347a455277339d8b8b32cfc17b8f2fbe65b584f4bda4c (Loader Inicial VBS)
- 1b848b6149d1c44bade82c6dc01aeeb2a1901305196dd032e6420ed2517add0f
- 2092e2a7d2cfa3bd102124276ecf96f6dd8f4c8113244c6481e839061c8c3f5e
- 325b30147b5fc16757d2f06659124606125768ca73ab360c149ef76ea881ac54
- 3fa723dd47839c3d13d4850095bed26b583bba1c37fbad48f1ba52906a4d20d5
- 574ebcfc0af38137fe635929388996b48766e313422bad82047fba18aa7925f0
- 66429129b8a4dffaf8ded0811ffc0499aa09444668101eb5ff405059efed646e
- 6b9058adee9aece15aef493ed86de10098d90dee84bcff09ae38553467a862a1
- 6ef786701b99b3b7f13ca0945ea9be3ee7d6c9b4b323e645a77a3425d607acc5
- 7245d8e35647271706b5b1c8cc65418884525d4ee8d783e900752d06f5ea0a2c
- 7b477bae4434684f2c0234443cd545e746d167d8b3e17c704abd6dec18c6eca3
- 93a8aa654d86af9d698cbd3c77ec7491b9f03475041c8b7421fe8dea17a13e7e
- 96ad1146eb96877eab5942ae0736b82d8b5e2039a80d3d6932665c1a4c87dcf7
- 97cf6ad52723e7701f3ef7ff032ac53a936df68968a3ecf8089d135f60e26cce
- 9843246cdc7f2399277bf9fd9de06f7846781a2a2fd9cd870915d6627d26a497
- 98867ae876989a5552c0db783f4bbfeda976ce81912bcff351d1be955eac964b
- 9b0f080307fd54f4dc9f7a8e6b841407165111e07b779c461f148225c98b2bbc
- a157030be7e03029123291b98462228465ced6dc686e4a9caeb9228739c73006
- a46e447b7c6a089af2d8f982c7b836719d49da77c5f88247dc932b5c5051d216
- a78aa83951940b474586bc025ea25b5770242ebcc3348ae273057365ebaf9221
- a7de5177c68a64bd48b36d49e2853799f4ebcfa8e4761f7cc472f333dc5f65cf
- ac7a2b93521fe6ca70d34277737199a3c26389f05d3ae0266e2359621e848ac7
- ba88cfeb854dfeeb4e2e77e20c2ce43982addb23d7001fd93ffa34d812b16806
- bcc6a4e05714f9d739e4d5d7f379c3443233f2fc38f44cd8eb4caf35c535733d
- bf7897c4f29dddb1a6a4e5056088b0aeefd0052e45fb43097b41b209e743ea80
- c00f5bfb56d0e2ee0ff1ca5f4cc02f72ebce1e402409ea28b0e0b81501ae9966
- d451b25024681de634aa41ef1127e38bc8e2874faebf38d0d0efddaaa7c0250f
- dd2a62e7a12d48c60a470378bd9f1c64d2616ceb2cc96102de67778a57959023
- e5026855466b29a088c4a11b57de7fa238318b82a15cc3565bd99c8c92c5c50c
- f0a62da9627a06bf0f46cae230cc0fea54c497bdb70fa51bcada775a5c167fc1
- f1945cd6c19e56b3c1c78943ef5ec18116907a4ca1efc40a57d48ab1db7adfc5
- ff7c266b906afdb3e2292e58c861c51d3f029f505ed825d0069daf2b305fb967

Direcciones IP

- 104.250.161.126
- 172.217.112.4
- 172.217.113.4
- 172.217.114.4
- 172.217.115.4
- 172.217.116.4
- 172.217.117.4
- 172.217.118.4
- 172.217.119.4

Recomendaciones Técnicas

- Deshabilitar wscript.exe / cscript.exe mediante directivas de grupo (GPO) para usuarios estándar.
- Implementar reglas de Reducción de Superficie de Ataque (ASR) que impidan a los motores de scripting del sistema lanzar binarios ejecutables o sesiones de PowerShell.
- Habilitar el registro detallado de bloques de código de PowerShell (Script Block Logging — Event ID 4104).
- Configurar reglas en el EDR para bloquear y alertar de forma inmediata cualquier intento de inyección o apertura de handles con permisos de lectura sobre el proceso lsass.exe.

Conclusión

La campaña descrita **representa una amenaza de nivel ALTO** para organizaciones colombianas de los sectores Gobierno, Financiero, Servicios Corporativos y Retail, materializada a través de un vector de ingeniería social (suplantación de CamScanner) que termina en el despliegue del troyano AsyncRAT con capacidades de robo de credenciales mediante intentos de acceso a la memoria de lsass.exe. El uso de infraestructura cloud legítima (Google Firebase) para el alojamiento del payload y de un proveedor de DNS dinámico (DuckDNS) para el C2 dificulta la detección basada exclusivamente en reputación de dominio, por lo que se recomienda priorizar controles de comportamiento (restricción de LOLBins, políticas de PowerShell, protección de LSASS) sobre mecanismos basados únicamente en listas negras o reputación estática.

Fuentes

AttackIQ. (2024, 24 de mayo). Emulating the open-source remote access Trojan (RAT) AsyncRAT.
https://www.attackiq.com/2024/05/24/emulating-asyncrat/
Cisco Talos. (2020, 29 de octubre). DoNot's Firestarter abuses Google Firebase Cloud Messaging to spread.
https://blog.talosintelligence.com/donot-firestarter/
CloudSEK. (2026, 27 de enero). AsyncRAT malware explained: Capabilities, risks, and detection.
https://www.cloudsek.com/knowledge-base/asyncrat-malware
eSentire. (2023, 13 de julio). Google Firebase Hosting abused to deliver Sorillus RAT, phishing page.
https://www.esentire.com/blog/google-firebase-hosting-abused-to-deliver-sorillus-rat-phishing-page
ESET. (2025, 15 de julio). Unmasking AsyncRAT: Navigating the labyrinth of forks. WeLiveSecurity.
https://www.welivesecurity.com/en/eset-research/unmasking-asyncrat-navigating-labyrinth-forks/
GBHackers. (2025, 7 de enero). New FireScam Android malware abusing Firebase services to evade detection.
https://gbhackers.com/firescam-malware-firebase/
Lakshmanan, R. (2025, 15 de julio). AsyncRAT's open-source code sparks surge in dangerous malware variants across the globe. The Hacker News.
https://thehackernews.com/2025/07/asyncrats-open-source-code-sparks-surge.html
Microsoft Threat Intelligence, & Microsoft Defender Experts. (2025, 21 de agosto). Think before you Click(Fix): Analyzing the ClickFix social engineering technique. Microsoft Security Blog.
https://www.microsoft.com/en-us/security/blog/2025/08/21/think-before-you-clickfix-analyzing-the-clickfix-social-engineering-technique/