Alerta

Reactivación del Troyano Bancario Grandoreiro en Latinoamérica

COLCERT AL – 20260826 - 116

TLP:CLEAR

Resumen Ejecutivo

NIVEL DE RIESGO

ALTO

Se identificó un resurgimiento activo del troyano bancario Grandoreiro, una amenaza que compromete críticamente a organizaciones en América Latina, con un foco particular de riesgo en México, Perú y Argentina, entre otros países de la región.

Esta amenaza, desarrollada en Delphi y activa desde al menos 2016, ha demostrado una alta resiliencia operativa. Tras la disrupción policial sufrida en 2024, su código fuente evolucionó hacia variantes más ligeras y evasivas; de hecho, la versión observada entre mayo y junio de 2026 cesó operaciones en Brasil y Portugal para concentrar estratégicamente su capacidad de ataque contra objetivos en México, el resto de LATAM y España.

Para materializar el compromiso, la campaña emplea un vector de entrega basado en correos maliciosos (malspam) que adjuntan un archivo ZIP camuflado como factura (ej. Fac-BH22DC0608_RevMQKSAC.zip). Posteriormente, la cadena de infección eleva el riesgo al abusar de la aplicación legítima Duplicate Files Finder (DFF) mediante la técnica de DLL side-loading, el ejecutable genuino es renombrado de forma aleatoria para cargar sigilosamente una DLL maliciosa (mingwm10.dll), logrando así evadir detecciones al ser ejecutada por un proceso de confianza.

Como contramedida frente a los controles de seguridad, antes de contactar a su servidor de Comando y Control (C2), el cargador ejecuta rigurosas validaciones anti-sandbox y anti-VM. Estas incluyen la verificación del tiempo de actividad, perfilado de hardware, detección de hipervisores (VMware, VirtualBox), inspección de 49 procesos de análisis, geolocalización condicional y validación de nombres de equipo contra listas negras; si alguna comprobación falla, el malware aborta la ejecución y despliega un falso mensaje de error en español, dificultando significativamente el análisis forense y la respuesta a incidentes.

Finalmente, para asegurar la descarga del payload de segunda etapa, la comunicación con el C2 se oculta utilizando DNS-over-HTTPS (DoH) de Google hacia el dominio malicioso (b7441561030408283960 40[.]nhlfan[.]net). Este tráfico se camufla mediante una solicitud HTTP GET cifrada a través del puerto TCP 6432 (usualmente asociado a PgBouncer), lo que, sumado a un esquema propietario de ofuscación de cadenas combinando Base64 y operaciones XOR, incrementa severamente la probabilidad de evadir los perímetros de seguridad tradicionales.

Contexto de la amenaza

Grandoreiro es un troyano bancario desarrollado en lenguaje Delphi, activo desde al menos 2016 e históricamente enfocado en mercados de habla portuguesa e hispana. Tras la acción policial internacional de 2024 contra sus operadores, la amenaza demostró una alta capacidad de adaptación, bifurcando su código fuente hacia variantes más ligeras y evasivas. De hecho, la versión analizada entre mayo y junio de 2026 marca un reajuste estratégico y un preocupante cambio de foco geográfico, cesó su actividad en Brasil y Portugal para concentrar su capacidad ofensiva directamente contra México, España y otros países de América Latina.

Ante este panorama, esta campaña representa un riesgo inminente y directo para Colombia, considerando que el sector financiero y bancario es su objetivo central de compromiso. La gravedad de la situación se agudiza al documentarse explícitamente que uno de los artefactos críticos del malware, el ejecutable alterado de Duplicate Files Finder ya ha sido detectado mediante telemetría en Colombia, lo que ratifica la existencia de actividades maliciosas y campañas de infección activas desplegándose actualmente sobre el territorio nacional.

Motivaciones y objetivos

La motivación subyacente de esta amenaza es de carácter estrictamente lucrativo. Grandoreiro opera como un troyano bancario diseñado específicamente para vulnerar credenciales críticas y exfiltrar activos, afectando tanto a la infraestructura de las organizaciones como a los usuarios finales. En consecuencia, el objetivo primordial y de máximo riesgo para esta reciente campaña recae de manera directa sobre las entidades del ecosistema financiero y bancario a lo largo de América Latina (LATAM).

Técnicas y Tácticas – MITRE ATT&CK

La tabla siguiente reproduce el mapeo de tácticas, técnicas e identificadores MITRE ATT&CK documentado

Táctica	ID	Técnica / Subtécnica	Detalle observado
Sigilo / Ejecución (Stealth / Execution)	T1574	Hijack Execution Flow	Carga de la DLL maliciosa mingwm10.dll a través del ejecutable legítimo de Duplicate Files Finder (DLL side-loading).
Sigilo / Descubrimiento (Stealth / Discovery)	T1497	Virtualization/Sandbox Evasion: System Checks	Verificación de tiempo de actividad del sistema (>180 segundos), detección de hipervisores, accesos directos y claves de BIOS.
Sigilo (Stealth)	T1564.003	Hide Artifacts: Hidden Window	Ocultamiento inmediato de la ventana de interfaz gráfica (GUI) del ejecutable DFF tras la carga lateral.
Sigilo (Stealth)	T1140	Deobfuscate/Decode Information	Rutina personalizada en memoria para desofuscar cadenas de texto mediante Base64 combinado con operaciones XOR.
Sigilo (Stealth)	T1036.005	Masquerading: Match Legitimate Resource Name or Location	Renombrado del binario benigno de Duplicate Files Finder a una cadena aleatoria para enmascaramiento.
Descubrimiento (Discovery)	T1082	System Information Discovery	Lectura de espacio libre en C:, número de CPUs, memoria RAM física y resolución de pantalla.
Descubrimiento (Discovery)	T1057	Process Discovery	Escaneo activo de 49 nombres de procesos correspondientes a depuradores, EDR y herramientas de análisis de red.
Descubrimiento (Discovery)	T1614	System Location Discovery	Consulta a ip-api[.]com y descarte de ejecución por geolocalización (observado: República Checa, Rusia, Países Bajos).

Táctica	ID	Técnica / Subtécnica	Detalle observado
Comando y Control (Command & Control)	T1071.001	Application Layer Protocol: Web Protocols	Solicitud HTTP GET cifrada sobre el puerto no estándar TCP 6432 para descargar el payload de segunda etapa.
Comando y Control (Command & Control)	T1071.004	Application Layer Protocol: DNS Resolution (DoH)	Uso de DNS-over-HTTPS de Google (dns.google) para resolver la dirección IP del servidor C2, ocultando la consulta DNS real.

Carga lateral de DLL (DLL Side-Loading)

- El malware explota la aplicación de confianza Duplicate Files Finder (DFF) utilizándola como vector principal de ejecución.
- El archivo original es renombrado de forma aleatoria para enmascarar su verdadero propósito operativo. Mediante análisis de telemetría en Colombia, se identificó el uso de este artefacto bajo el nombre _2IH4ENJIRRNCobran_03732qyykae214BKXXN6180-Dt.exe.
- Al ser detonado, el programa legítimo inicia su proceso siguiendo estrictamente el orden estándar de búsqueda de bibliotecas dinámicas (DLL) del sistema operativo Windows.
- Los atacantes aprovechan este comportamiento ubicando estratégicamente una DLL maliciosa en el mismo directorio local que el ejecutable, disfrazándola deliberadamente con el nombre de una dependencia real del sistema (mingwm10.dll).
- La aplicación de confianza carga la DLL maliciosa en su propio proceso, permitiendo que el código del malware se ejecute de manera sigilosa, haciéndose pasar por parte de un software legítimo.
- Engañada por la jerarquía de directorios, la aplicación genuina carga el código malicioso directamente en su propio espacio de memoria. Esto permite que el malware opere de manera altamente sigilosa, consolidando el compromiso bajo la fachada de un proceso seguro y legítimo.

Evasión de análisis y detección (Anti-Sandbox / Anti-VM)

Antes de realizar cualquier actividad maliciosa o contactar a su servidor de Comando y Control (C2), el cargador valida si se encuentra en un entorno de usuario real o en un sistema de análisis, mediante las siguientes comprobaciones:

- Tiempo de actividad del sistema: verifica que el sistema lleve funcionando al menos tres minutos (180 segundos), buscando evadir sandboxes que inician el análisis desde un estado recién arrancado.
- Comprobación de software instalado: busca accesos directos específicos en el escritorio (Chrome, CCleaner, Firefox, FileZilla, Acrobat Reader, Edge, Skype). La presencia simultánea de todos estos programas se interpreta como indicador de un entorno de análisis preconfigurado, y detiene la ejecución.
- Perfilado del entorno (profiling): recopila memoria física, número de procesadores, espacio libre en disco, resolución de pantalla y actividad reciente del usuario.
- Detección de artefactos de virtualización: busca controladores y componentes de software específicos de VMware y VirtualBox (archivos .sys y .dll), y revisa registros de la BIOS en busca de palabras clave como VBOX, VMWARE, VIRTUAL, QEMU, XEN.

- Inspección de procesos en ejecución: revisa la lista de procesos activos (49 nombres de procesos) buscando herramientas de depuración, ingeniería inversa, análisis de red y monitoreo de seguridad (p. ej. procmon, Wireshark, depuradores, desensambladores); detiene la ejecución si detecta alguna.
- Geolocalización y bloqueo de países: se conecta al servicio externo ip-api[.]com para determinar la dirección IP pública y la ubicación, bloqueando la ejecución en ciertos países (observado en la fuente: República Checa, Rusia y Países Bajos) para evitar entornos de investigadores o sandboxes automatizados.
- Validación de nombres de usuario y equipo: compara el nombre del usuario actual y del host contra una lista negra interna, incluyendo cuentas predeterminadas de Windows Sandbox.

Si alguna de estas comprobaciones falla, el malware detiene su ejecución y puede mostrar un mensaje de error simulado en español para despistar al usuario. La fuente documenta un ejemplo concreto: un cuadro de diálogo con apariencia de Adobe Reader que muestra el texto “Hubo un error al ver su documento, reinicie su computadora y vuelva a intentarlo.”, con botón de confirmación “OK”.

Indicadores de Compromiso (IoCs) Hashes de archivo

Artefacto	Hashes	Contexto
Fac-BH22DC0608_RevMQKSAC.zip	SHA256: cc238813ab277cbb4324d37875c37985ca5baeaf8c412b4c85aa8ec5faec7096 SHA1: 7fa480b8a7dbcc1ce826d1cd6b82d5ee75552484 MD5: 82f771c3ec4fe979c3ae00372e8c3ac8	ZIP inicial de la campaña, distribuido con nombre engañoso similar a una factura (posible vector de phishing/spam).
_2IH4ENJIRRNCobran_03732qyykae214BKXXN6180-Dt.exe	SHA256: 98e56c5f902fb825f6f122122ba6a2a0febee1e582a462f74dd1d99b018bf7c0 SHA1: 7bc79e8bbff363b41fd73f9bea102ddc4a404cbe MD5: cfbd8d062e9baa98737a0260996f48c6	Ejecutable legítimo de Duplicate Files Finder renombrado aleatoriamente; identificado mediante telemetría en Colombia.
dupfdll.dll	SHA256: fad1e9d507c7021a62998a547ab53b3ee438846f7ae753285fdb3917dd2dcdfa SHA1: e6ae8be61928e1279190b0df28ac8ad94f3ac29d MD5: e882ee4a643b00871c98bcfe4b4d7cd1	DLL legítimo intermedio (BENIGNO), parte de la herramienta Duplicate Files Finder; utilizado para realizar la técnica de DLL side-loading.
mingwm10.dll	SHA256: 90254c3baec79cf9b448836293d3864ee273c30de374933296c6e8e3bcaefdbd SHA1: 077b104db18e1c1fdd0800e6e75a1e26398d97e7 MD5: f1aed8cf2adafa86927fc58d5f24073e	DLL maliciosa inyectada mediante side-loading; ejecuta la lógica principal del cargador de Grandoreiro.

Indicadores de red

Tipo	Valor / Indicador	Contexto
URL	hxxps://dns[.]google/resolve?name=<dominio C2>	Solicitud HTTP cifrada hacia el servicio DNS-over-HTTPS (DoH) de Google, utilizada para resolver el dominio C2 ocultando la consulta DNS real.
Dominio (C2)	b744156103040828396040[.]nhlfan[.]net	Dominio de comando y control (C2) predefinido, resuelto vía DoH.
Puerto	TCP / 6432	Puerto utilizado para la comunicación C2 (descarga de payload de segunda etapa). Nota de la fuente: este puerto suele emplearse legítimamente por PgBouncer (administrador de conexiones para bases de datos PostgreSQL), lo que puede dificultar su identificación en el tráfico de red.
Dominio (servicio externo)	ip-api[.]com	Servicio externo consultado por el malware para validar la IP pública del equipo infectado y determinar su ubicación geográfica antes de proceder.

Recomendaciones técnicas

Las siguientes recomendaciones se formulan a partir de la cadena de infección, las técnicas MITRE ATT&CK y los indicadores de compromiso documentados.

Filtrado de correo y control de archivos adjuntos (frente al vector de entrega)

- ❑ Bloquear o poner en cuarentena archivos ZIP adjuntos a correos no solicitados, especialmente aquellos con nombres que simulan facturas o documentos financieros.
- ❑ Aplicar reglas de detección de archivos ejecutables (.exe) empaquetados dentro de archivos ZIP recibidos por correo.

Detección de DLL Side-Loading (frente a T1574, T1036.005)

- ❑ Monitorear la carga de DLLs no firmadas o firmadas de forma inconsistente por procesos de aplicaciones legítimas como Duplicate Files Finder.
- ❑ Aplicar control de aplicaciones (application allowlisting) que restrinja la ejecución de binarios renombrados o no reconocidos, especialmente aquellos con patrones de nombre aleatorios similares al observado (_2IH4ENJIRRNCobran_03732qyykae214BKXXN6180-Dt.exe).
- ❑ Habilitar auditoría de carga de módulos (Sysmon Event ID 7 – Image Loaded) para detectar el orden de búsqueda de DLL abusado por esta técnica.

Detección de comportamiento anti-sandbox / anti-VM (frente a T1497, T1082, T1057)

- ❑ Configurar los entornos de sandbox y análisis dinámico corporativos para simular un tiempo de actividad del sistema superior a 180 segundos antes del análisis, y para no depender exclusivamente de la ausencia de software de usuario común.
- ❑ Monitorear procesos que enumeren de forma masiva y sistemática la lista de procesos en ejecución en un corto periodo de tiempo, como indicador de comportamiento anti-análisis.
- ❑ Auditar consultas al registro de Windows relacionadas con claves de BIOS y palabras clave de virtualización (VBOX, VMWARE, VIRTUAL, QEMU, XEN) desde procesos no administrativos.

Detección de red (frente a T1071.001, T1071.004, T1614)

- ❑ Inspeccionar y alertar sobre tráfico saliente hacia el dominio C2 b7441561030408283960 40[.]nhlfan[.]net y sobre solicitudes DoH a dns.google que incluyan patrones de subdominio numérico similares.
- ❑ Monitorear conexiones salientes sobre el puerto TCP 6432 hacia destinos externos no asociados a infraestructura de bases de datos PostgreSQL/PgBouncer conocida y autorizada por la organización.
- ❑ Alertar sobre conexiones salientes hacia ip-api[.]com desde estaciones de trabajo o servidores que no tengan una necesidad de negocio documentada para servicios de geolocalización de IP.
- ❑ Donde sea posible, inspeccionar el tráfico DoH corporativo o restringir el uso de resolutores DoH de terceros no autorizados, para mantener visibilidad sobre las resoluciones DNS reales.

Hardening y control de endpoint

- ❑ Mantener actualizadas las soluciones EDR/XDR y verificar su resiliencia frente a técnicas de ocultamiento de ventana y masquerading de binarios legítimos renombrados.
- ❑ Restringir la instalación y ejecución de utilidades de terceros como Duplicate Files Finder en estaciones de trabajo del sector financiero mediante políticas de control de aplicaciones, o validar la integridad de sus binarios mediante firma digital antes de la ejecución.

Conclusión

El resurgimiento del troyano Grandoreiro, con un foco estratégico en México, España y otros países de América Latina representa una amenaza con un nivel de impacto Alto para el sector financiero y bancario. La gravedad de esta alerta se acentúa a nivel local, dado que los análisis de telemetría ya han confirmado la presencia activa de sus artefactos maliciosos en Colombia.

La combinación de un vector de entrega basado en ingeniería social (malspam con archivos ZIP que simulan facturas), la explotación de software legítimo mediante la técnica de DLL Side-Loading y la implementación de un sofisticado conjunto de validaciones anti-sandbox y anti-VM, evidencia una operación altamente especializada. Esta campaña está diseñada de manera específica para evadir tanto los controles automatizados de seguridad como las labores de análisis manual y forense por parte de los investigadores

Fuentes

Google. (s. f.). Google Threat Intelligence. Google Cloud
https://cloud.google.com/security/products/threat-intelligence

Google. (s. f.). VirusTotal
https://www.virustotal.com/

MITRE. (s. f.). MITRE ATT&CK®.
https://attack.mitre.org/