

Resumen Ejecutivo

El Equipo de Respuesta a Emergencias Cibernéticas de Colombia (ColCERT) ha analizado una campaña sobre una posible exfiltración información de entidades públicas e instituciones de educación superior en Colombia, registrando al menos 23 reportes de seguridad digital atribuidos a 9 actores de amenaza distintos durante el primer trimestre del año.

El actor de amenaza predominante, identificado, es responsable de la mayor parte de los reportes generados, identificando que su modo de operación se centra en la exfiltración y publicación de conjuntos de datos de identificación básica (nombres, correos institucionales, fotos de perfil), presuntamente obtenidos a través de la explotación de vulnerabilidades conocidas y de día cero, o por malas configuraciones en plataformas de Sistema de Gestión del Aprendizaje como Moodle y aplicaciones Legacy, entre otras.

Esta campaña representa un riesgo significativo para la reputación de las entidades afectadas y para la confidencialidad de la información institucional. La información expuesta, aunque fragmentada, puede ser utilizada para ejecutar ataques de ingeniería social, phishing dirigido (spear-phishing) y suplantación de identidad.



Hallazgos técnicos relevantes:

El análisis del material compartido en las publicaciones permite identificar varios elementos técnicos relevantes:

- ❑ Los archivos difundidos se presentan principalmente en formatos de texto plano, donde los registros aparecen listados de manera secuencial con un número limitado de campos.
- ❑ Los datos observados corresponden principalmente a nombres, apellidos, correos electrónicos institucionales y, ocasionalmente, fotografías de perfil.
- ❑ Aunque el actor se refiere al material como “database”, los archivos no presentan estructuras propias de exportaciones de bases de datos SQL, como esquemas de tablas, delimitadores consistentes o relaciones entre registros.
- ❑ En algunos casos se mencionan “códigos de estudiante”, sin embargo, los valores observados corresponden a números muy cortos (uno o dos dígitos), lo que resulta atípico para identificadores institucionales diseñados para identificar de manera única a usuarios dentro de sistemas académicos.
- ❑ También se han observado repositorios con grandes volúmenes de imágenes tipo retrato, que no contienen metadatos ni información identificable dentro de los archivos que permita vincularlas directamente con registros específicos.
- ❑ Estos elementos sugieren que las muestras publicadas corresponden principalmente a colecciones de información desagregada o fragmentos de datos, más que a exportaciones completas de bases de datos institucionales.

Patrones detectados y tendencias observadas

- ❑ **Focalización sectorial:** Existe una clara concentración de ataques en el sector educativo y el sector gubernamental. Esto sugiere que los actores han identificado una debilidad común o una superficie de ataque recurrente en estas entidades.
- ❑ **Explotación de plataformas:** La hipótesis del compromiso de plataformas LMS como vector de entrada principal para NyxarGroup es consistente con el tipo de datos filtrados y el perfil de las víctimas. Estas plataformas, a menudo gestionadas con recursos limitados, pueden presentar vulnerabilidades no parcheadas o configuraciones de privacidad permisivas.
- ❑ **Modelo de "Leak-to-Sell":** El patrón de publicar muestras gratuitas para luego ofrecer el conjunto de datos completo a la venta es una táctica común para actores que buscan tanto reputación como beneficio económico.
- ❑ **Baja complejidad técnica aparente:** La naturaleza de los datos filtrados (listados simples) sugiere que los ataques podrían no requerir técnicas altamente sofisticadas, sino más bien la explotación de fallos de seguridad básicos como la falta de actualizaciones, contraseñas débiles o una gestión inadecuada de la visibilidad de la información.

Hipótesis técnica

Una de las entidades mencionadas en las publicaciones del actor identificó indicios que sugieren la posible interacción con plataformas de gestión de aprendizaje (Learning Management Systems – LMS) utilizadas por instituciones educativas. El tipo de información observada en las publicaciones, nombres, apellidos, correos institucionales y fotografías de perfil infieren que podrían tratarse de información de perfiles de usuario en plataformas LMS, como Moodle u otras soluciones similares.

Bajo esta hipótesis, el actor posiblemente este explotando vulnerabilidades conocidas y de día cero, así mismo utilizando credenciales exfiltradas, recopilando información de perfiles de usuario como por ejemplo de plataformas educativas, lo que explicaría tanto la naturaleza limitada de los datos observados como la presencia ocasional de fotografías asociadas a perfiles académicos, para la identificación de vulnerabilidades conocidas podría estar utilizando técnicas OSINT o Google Dorks, lo que permite identificar puertos, infraestructura desplegada en sitios web, encabezados, documentos y sistemas operativos.

Perfil del actor principal

NyxarGroup es un actor emergente dentro de los ecosistemas clandestinos de filtración y comercialización de información, cuya actividad reciente ha estado caracterizada por la publicación de supuestos conjuntos de datos asociados a organizaciones de distintos sectores. A diferencia de otros tipos de ataques que priorizan la interrupción operativa, parece centrarse en la exposición y difusión de información presuntamente obtenida de entornos institucionales, lo que sugiere un modelo de operación orientado a la generación de visibilidad, reputación dentro de comunidades clandestinas y potencial monetización de datos.

El actor utiliza foros clandestinos orientados a la divulgación de filtraciones de datos para publicar información asociada a diferentes organizaciones. Las publicaciones siguen un formato relativamente consistente, que incluye:

- Un título que identifica el país y el dominio institucional afectado.
- Un mensaje introductorio dirigido a la comunidad del foro.
- Una breve descripción del tipo de información supuestamente obtenida.
- La inclusión de imágenes o logotipos de la institución mencionada.
- Enlaces a repositorios de descarga o contenido oculto dentro del foro.

El análisis de los archivos compartidos por NyxarGroup permite identificar ciertas inconsistencias entre la forma en que el actor describe la información en sus publicaciones y la estructura real de los datos disponibles en los conjuntos difundidos. Aunque en los anuncios realizados dentro del foro el actor suele referirse al material como una “database”, el contenido observado no presenta las características propias de una base de datos relacional exportada desde sistemas como MySQL, PostgreSQL u otros motores SQL.

En los archivos analizados, la información se encuentra organizada principalmente en archivos de texto plano, donde los registros aparecen listados de manera secuencial y con un número limitado de campos.

Estos registros suelen incluir un valor numérico inicial, seguido por un nombre y, en algunos casos, otros elementos de identificación como correos electrónicos institucionales. No obstante, la estructura general del archivo no evidencia esquemas, delimitadores consistentes, ni metadatos que permitan identificar tablas, relaciones entre registros o estructuras típicas de exportaciones de bases de datos.

En algunos casos, el acceso a los archivos se encuentra disponible mediante enlaces directos a servicios de almacenamiento público, mientras que en otras publicaciones el contenido se encuentra oculto mediante mecanismos internos del foro que requieren el pago de créditos de la plataforma para visualizar los enlaces de descarga.



Asimismo, el actor ha reconocido en algunas publicaciones que su reputación dentro del foro aún es limitada y que ciertos miembros de la comunidad han expresado dudas sobre la legitimidad de las filtraciones anunciadas. En respuesta a estos cuestionamientos, el actor ha publicado muestras adicionales con el objetivo de reforzar la credibilidad de sus afirmaciones.

Este patrón refuerza la evaluación de que el material compartido públicamente consiste principalmente en colecciones de registros desagregados o fragmentos de información, más que en repositorios estructurados directamente extraídos de bases de datos institucionales completas.

Recomendaciones estratégicas y buenas prácticas

Con base en el análisis realizado, se establecen las siguientes recomendaciones estratégicas y acciones prioritarias con el objetivo de fortalecer la postura de seguridad institucional y mitigar el riesgo de futuras exfiltraciones de información.

- Acciones Prioritarias Inmediatas
- Auditoría de Registros de Acceso
- Actualización y Parcheo de Sistemas
- Restricción de Visibilidad de Perfiles
- Implementación de Autenticación Multifactor (MFA)
- Revisión de Políticas de Autenticación
- Hardening de Sistemas

Estrategias de fortalecimiento continuo

1. Gestión de identidad y control de credenciales

- Rotación de credenciales
- Prevención de infecciones por Infostealer y Monitoreo de "Infostealer Logs"
- Autenticación Adaptativa

2. Reducción de la Superficie de Ataque (Mitigación OSINT)

- Gestión y Auditoría Continua de Activos
- Higiene de Repositorios Públicos
- Evaluación de Exposición de Información

3. Gestión de Vulnerabilidades y Configuraciones

- Programa de escaneo de vulnerabilidades
- Análisis basado en riesgo
- Seguridad en la nube y SaaS

4. Detección y respuesta a incidentes

- Monitoreo de anomalías
- Detección de archivos con listados de usuarios/correos generados automáticamente sin autorización.
- Solicitudes secuenciales a endpoints de perfil de usuario o API de directorio en períodos cortos (scraping).
- Actividad de cuentas con privilegios en horarios inusuales o desde geolocalizaciones inconsistentes.
- Menciones de los dominios de la entidad en foros clandestinos o plataformas de leakage.
- Planes de Respuesta a Incidentes

5. Concientización y Capacitación

- Programas de Concientización continua

Fuentes

- Monitoreo de fuentes abiertas de información.
- Equipo de ciberseguridad de la Universidad del Rosario
- Equipo de seguridad de la Universidad UNAD
- Equipo de seguridad de la DIAN