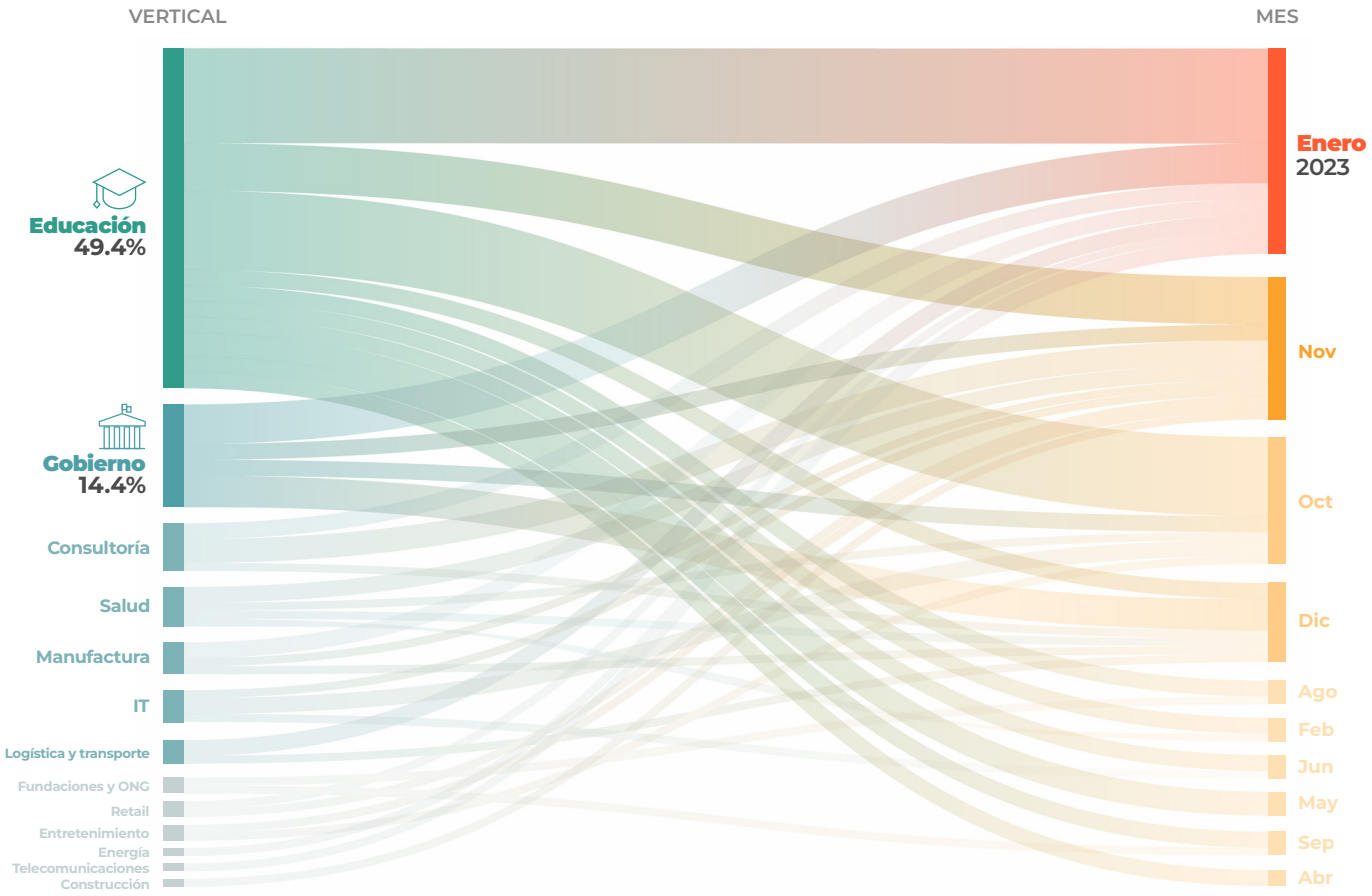
Lumu detecta incremento en la comercialización de credenciales de acceso a Office 365 y dominios de internet en Colombia

El estado de la seguridad cibernética en Colombia ha tomado una preocupante vuelta en los últimos meses con varias empresas sufriendo importantes disrupciones en sus operaciones de negocios.

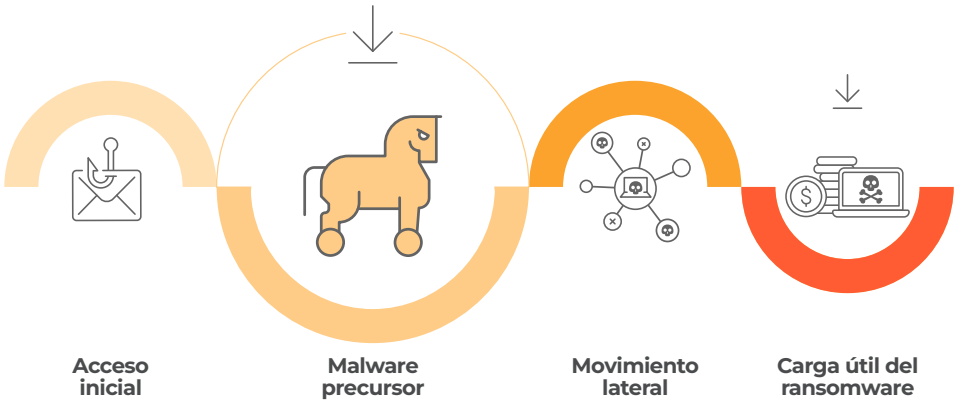
La comercialización de credenciales de acceso ha probado ser muy útil a los grupos de ciberdelincuencia ya que sirven como una forma eficaz de entrar a las organizaciones. Particularmente en Colombia, en 2023 Lumu observa un **incremento del 1200%** en la comercialización de credenciales de acceso a cuentas de correo electrónico comparado con el mismo periodo del año anterior. Esto sin duda ubica al país y a los ciudadanos ante un panorama en que los ataques de Ransomware y brechas de ciberseguridad continuarán en aumento.



Comparación entre verticales de la industria más afectadas por credenciales comprometidas de Office 365 con respecto a 2022 y enero de 2023.

¿Qué tipo de ataques se pueden generar en este contexto?

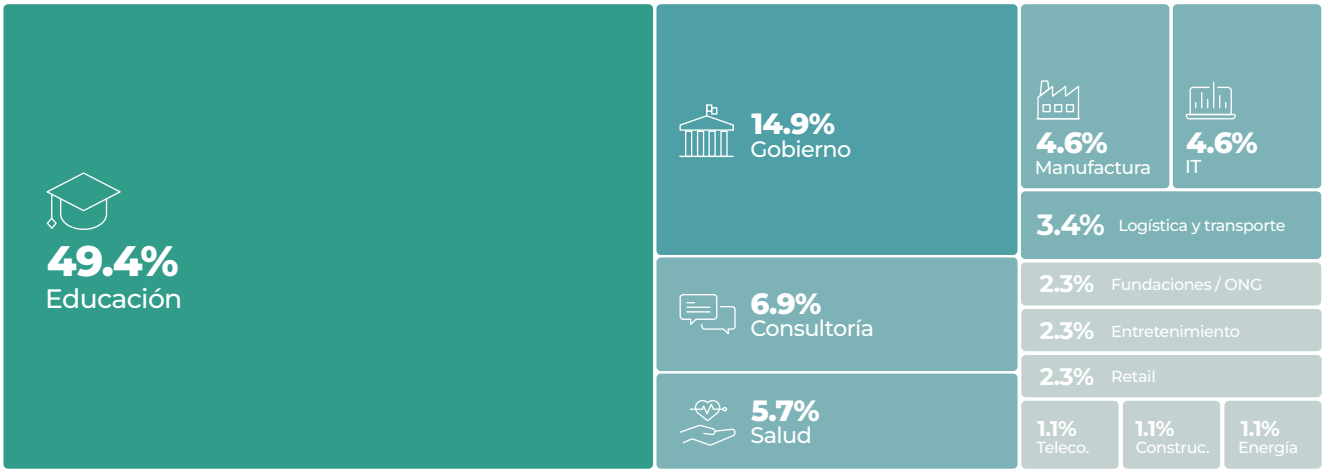
Los ataques de Ransomware o de secuestro de datos y brechas de seguridad no aparecen de la nada, típicamente inician con el compromiso de credenciales de acceso a sistemas de infraestructura o correo electrónico.



Cadena de eventos que típicamente anteceden un ataque de Ransomware.

A día de hoy, los principales afectados por esta venta de credenciales de acceso son entidades de gobierno e instituciones educativas en todo el país. La gravedad de esta situación radica en que cada vez que los atacantes toman control de una cuenta de correo electrónico, esta se convierte en un vector de distribución de Phishing para instalar Malware precursor en los sistemas de otras organizaciones. La efectividad de estos ataques está determinada por la capacidad de usar una cuenta legítima con la que pueden engañar a más usuarios. Un ejemplo de ello son los correos que advierten de una multa de tránsito, o un proceso judicial en curso e inducen al usuario a descargar el archivo del comparendo, una vez efectuada la descarga y se instala el malware precursor, se abre la puerta a un ataque de ransomware o filtración de información confidencial.

¿Actualmente cuáles son los tipos de entidades más expuestas?



Principales industrias afectadas por el compromiso de credenciales de acceso.

Cuentas de correo comprometidas

Nuestro equipo de inteligencia de amenazas ha detectado por lo menos **80 organizaciones** de diferentes tamaños y sectores de la industria, para las que los delincuentes ya cuentan con puertas de entrada a través del correo electrónico.

El análisis de nuestros expertos ha determinado que las instituciones de educación y entidades de gobierno son las más expuestas a sufrir un ataque de ransomware o brecha de datos y así mismo son las entidades que más probablemente serán usadas como un puente para comprometer la infraestructura de otras organizaciones.

Tan sólo en enero de 2023 van **27 organizaciones** para las que hemos detectado credenciales comprometidas que permiten acceso a la plataforma de correo de Office 365 usadas por las organizaciones afectadas. De las 27 identificadas, **17 pertenecen al sector gobierno e instituciones de educación**.

Educación

- ipn.edu.co
- colegioaleman.edu.co
- iser.edu.co
- ipn.edu.co
- unipamplona.edu.co
- cbsjd.edu.co
- unadvirtual.edu.co
- unipamplona.edu.co
- uco.edu.co
- escolme.edu.co
- uac.edu.co
- udenar.edu.co
- marymountbq.edu.co
- ulibertadores.edu.co

Gobierno

- fiscalia.gov.co
- uaesp.gov.co
- personeriabogota.gov.co
- lebrija-santander.gov.co
- mincit.gov.co

Dominios de internet comprometidos

Hemos identificado por lo menos **25 dominios** de internet pertenecientes a marcas y/o compañías de diferentes verticales de la industria en Colombia, que han sido comprometidos por cibercriminales y cuyas credenciales de administración están siendo comercializadas. Adicionalmente, dentro de los factores comunes a estos dominios, se destaca que todos son administrados a través de la reconocida plataforma cPanel. La criticidad de esta situación radica en que los atacantes podrían aprovecharse de estos dominios legítimos para crear subdominios, carpetas, y servidores de correo, que les permita generar nuevos ataques de phishing con mayor alcance y efectividad. Adicionalmente, mediante esta técnica, los ciberdelincuentes suelen hospedar enlaces maliciosos que llevan a la descarga de malware precursor que abre el camino a posteriores ataques de ransomware o brechas de seguridad.

- clioftalcar.com
- ftstecnologia.com.co
- hydraulicforcesas.com.co
- consorcioodi.com
- ingeproplus.com
- nexumservicios.com
- sarriarealpe.com
- jorgeiglesiasmarquez.com
- micdotaciones.com
- sercomexsas.com
- savannaflowers.com.co
- hyesas.com
- serandes.com
- impact-psy.com
- gapingenieria.com
- fundacionelprogresojs.org
- kairossystems.com.co
- conserjesinmobiliarios.com.co
- setelin.co
- districtre.com
- escueladelogistica.edu.co
- consultor.syso.co
- olglass.co
- custom-pet.com
- pestcontrolltda.com
- horusseguridad.com
- sintrasersalud.com

¿Qué pueden hacer las organizaciones en Colombia para defenderse ante este panorama?

- **Cerrar la puerta a nuevos atacantes -** Es importante que las organizaciones lleven a cabo un proceso en el que sus empleados y proveedores realicen la actualización de credenciales de acceso a los diferentes sistemas corporativos. Adicionalmente se recomienda la activación de un segundo factor de autenticación obligatorio para el inicio de sesión.
- **Identificar la presencia de adversarios en su red -** El análisis de metadatos de red (Registros DNS, proxy, Firewall, y netflow) es una herramienta fundamental para identificar activos informáticos que estén tratando de contactar dominios controlados por adversarios.
- **Comprobar si ya han intentado vulnerar su seguridad -** Analizar el contenido de las bandejas de correo electrónico incluyendo las casillas de SPAM es fundamental para comprobar si a sus empleados ya ha llegado correo malicioso enviado desde dominios de empresas comprometidas. No basta con bloquear el SPAM, es necesario analizar su contenido para entender cómo afinar la estrategia de defensa e identificar las tácticas que estén siendo utilizadas por ciberdelincuentes para engañar a sus colaboradores.
- **Validar los mecanismos de seguridad de su dominio web -** Es urgente cambiar las credenciales de acceso a las plataformas de administración web. Si bien dentro de los dominios comprometidos se identifica el uso de cPanel como un factor común, los administradores de sitios web gestionados a través de otras plataformas deberían aplicar esta recomendación.
- **Erradicar efectivamente el compromiso -** No es suficiente con bloquear los contactos generados hacia dominios controlados por atacantes. Se debe erradicar el compromiso que genera dichos contactos. Este mismo principio ayuda a reducir también el riesgo a sufrir brechas de datos que involucren la filtración de información confidencial.