Grandes compañías bajo amenaza: así operan los grupos de ransomware que secuestran información empresarial

julio 26, 2026 11:37 pm

Escuchar Noticia

Los ataques de ransomware continúan consolidándose como una de las mayores amenazas para empresas de todo el mundo. En los últimos meses, organizaciones de distintos sectores han reportado accesos no autorizados, robo de información y amenazas de publicación de datos confidenciales por parte de grupos especializados en extorsión digital.

Uno de los casos recientes que generó preocupación en Colombia involucró al Grupo Ecopetrol, luego de que la compañía confirmara un incidente de seguridad en el que un actor externo obtuvo acceso a recursos digitales y logró extraer información asociada a aproximadamente 3.300 cuentas de usuarios. El ataque también involucró entornos de almacenamiento en la nube de cerca de 15 compañías pertenecientes al grupo empresarial.

Aunque la petrolera aseguró que sus mecanismos de protección permitieron bloquear el intento de cifrado masivo característico del ransomware, el incidente evidenció la capacidad de estas organizaciones criminales para infiltrarse en infraestructuras empresariales altamente protegidas.

¿Qué ocurrió con la red de ransomware?

DIARIO DEL CAUCA

Contáctanos:
3138282538 - 3138284745

Los grupos modernos de ransomware ya no se limitan únicamente a bloquear archivos mediante cifrado y exigir un pago para recuperarlos. Actualmente utilizan una estrategia conocida como **doble extorsión**, que consiste en:

1. Ingresar de manera ilegal a los sistemas de una organización.
2. Extraer información confidencial antes de activar el ataque.
3. Amenazar con publicar los datos robados si la empresa no paga.
4. Presionar económicamente mediante sitios clandestinos donde anuncian a sus víctimas.

Este modelo ha convertido al ransomware en un negocio criminal organizado, donde existen grupos con diferentes integrantes especializados en infiltración, desarrollo de malware, negociación y publicación de información robada.

Uno de los grupos señalados en ataques recientes contra organizaciones internacionales es **The Gentlemen**, una operación de ransomware que, según reportes especializados, ha utilizado técnicas avanzadas para acceder a redes empresariales, extraer información y ejercer presión mediante amenazas de filtración.

Filtración de datos: el nuevo objetivo de los ciberdelincuentes

Durante años, el objetivo principal del ransomware era bloquear archivos internos para detener la operación de una compañía. Sin embargo, los atacantes han cambiado su estrategia: ahora buscan principalmente robar información valiosa.

Entre los datos que suelen convertirse en objetivo están:

- Bases de datos de clientes.
- Información financiera.
- Contratos empresariales.
- Documentos internos.
- Credenciales de empleados.
- Información almacenada en servicios de nube.

El valor de estos datos no solo está en venderlos en mercados ilegales, sino también en utilizarlos para chantajear a las compañías afectadas.

En el caso de Ecopetrol, la compañía informó que el incidente estuvo relacionado con extracción de información y un intento de ejecución de ransomware, aunque los controles internos permitieron contener la amenaza antes de que afectara completamente sus sistemas.

¿Cómo logran entrar los grupos de ransomware?

Aunque muchas personas imaginan que estos ataques requieren técnicas extremadamente sofisticadas, en numerosos casos los delincuentes aprovechan errores comunes dentro de las empresas.

Entre las principales puertas de entrada están:

1. Contraseñas débiles o reutilizadas

Los atacantes pueden obtener credenciales filtradas en ataques anteriores y utilizarlas para acceder a sistemas empresariales.

2. Fallas en accesos remotos

Servicios como conexiones VPN, escritorios remotos o plataformas administrativas pueden convertirse en puntos vulnerables si no cuentan con una configuración adecuada.

3. Correos fraudulentos

El phishing sigue siendo una de las técnicas más utilizadas. Los empleados reciben mensajes aparentemente legítimos que buscan robar contraseñas o instalar programas maliciosos.

4. Sistemas sin actualizar

Los equipos que mantienen versiones antiguas de software pueden contener vulnerabilidades conocidas que los atacantes aprovechan.

Recientemente, investigadores de Kaspersky alertaron sobre ataques en Colombia y México donde grupos de ransomware aprovecharon configuraciones incorrectas y herramientas legítimas del sistema para comprometer organizaciones. En algunos casos incluso utilizaron impresoras corporativas para imprimir las notas de rescate después de tomar control de los equipos.

El impacto para las empresas víctimas

Un ataque de ransomware puede generar consecuencias económicas y operativas importantes.

Entre los principales daños se encuentran:

Interrupción de servicios

Cuando una empresa pierde acceso a sus sistemas, puede detener procesos internos, atención al cliente o actividades comerciales.

Pérdida de confianza

La filtración de datos personales puede afectar la reputación de una compañía y generar preocupación entre clientes y empleados.

Costos de recuperación

Las organizaciones deben invertir en análisis forense, recuperación de información, fortalecimiento de seguridad y posibles procesos legales.

Riesgo regulatorio

Las empresas que manejan información personal pueden enfrentar investigaciones por no aplicar medidas suficientes de protección de datos.

En Colombia, la Superintendencia de Industria y Comercio ha ordenado medidas de seguridad adicionales después de incidentes relacionados con ataques ransomware, como ocurrió con IFX Networks Colombia tras un ataque externo que comprometió máquinas virtuales y servicios tecnológicos.

Empresas aumentan sus defensas ante una amenaza creciente

Ante el aumento de ataques, especialistas en seguridad recomiendan que las organizaciones adopten medidas preventivas como:

- Implementar copias de seguridad independientes.
- Activar autenticación multifactor.
- Capacitar empleados contra ataques de phishing.
- Actualizar constantemente sistemas y aplicaciones.
- Monitorear accesos sospechosos.
- Crear planes de respuesta ante incidentes.

Las copias de seguridad continúan siendo una de las herramientas más importantes, ya que permiten recuperar información sin depender del pago exigido por los atacantes.

Una amenaza que seguirá evolucionando

El ransomware dejó de ser un problema exclusivo de grandes empresas tecnológicas y ahora afecta sectores estratégicos como energía, salud, finanzas, manufactura y servicios públicos.

La tendencia muestra que los ciberdelincuentes buscan organizaciones con grandes volúmenes de información y estructuras complejas, donde una interrupción puede generar pérdidas millonarias.

La ciberseguridad dejó de ser únicamente un asunto del departamento de tecnología: actualmente representa un elemento estratégico para la continuidad y supervivencia de cualquier organización moderna.

ANTERIOR
¿Cuando y donde será la próxima velada del año?

SIGUIENTE
Mientras crecen los traslados hacia Colpensiones, más de 9.000 trab...

Te Puede Interesar

Charli XCX lanza 'Music, Fashion, Film: Nueva apuesta por el rock, las guitarras y colaboraciones

27 julio, 2026 /// No hay comentarios

La Secretaría Distrital de Integración Social transforma la vida de más de 5.600 jóvenes

27 julio, 2026 /// No hay comentarios

Boca Juniors, con Montero y Villa, fue goleado por el modesto Riestra en Argentina

27 julio, 2026 /// No hay comentarios

El Teatro El Ensueño recibe el concierto 'Flores del Asfalto'

27 julio, 2026 /// No hay comentarios


HERNANDO SUÁREZ BURGOS
PROPIETARIO CADENA DE ALMACENES LUBER
984