El ransomware asciende en el organigrama: los directivos son objetivos prioritarios

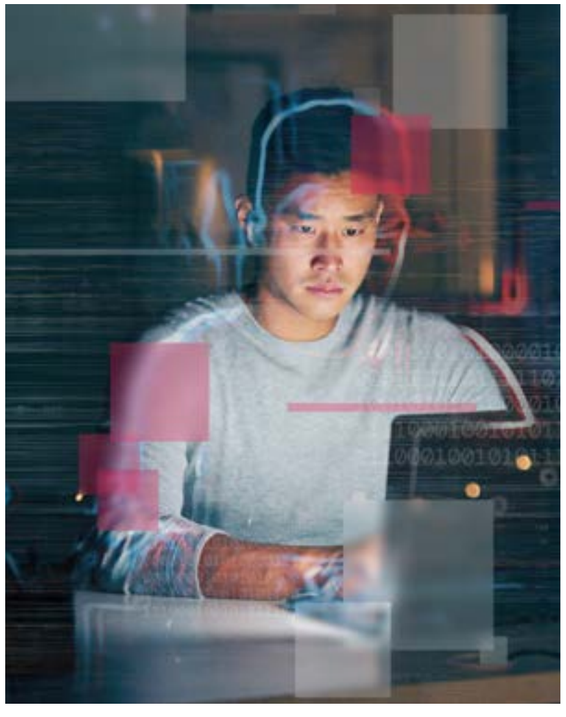
zscaler™

INVESTIGACIÓN DE THREATLABZ

Los informes sobre ataques de ransomware suelen centrarse en las empresas que sufren brechas de seguridad, los datos robados, las herramientas de malware y los pagos de rescates. Sin embargo, apenas hay datos sobre las personas a las que atacan los ciberdelincuentes dentro de las organizaciones. Una nueva investigación de ThreatLabz cubre esta laguna y examina el factor humano de los ataques de ransomware, incluidos los cargos y las funciones empresariales más representados entre las víctimas. Los resultados revelaron que los ciberdelincuentes que emplean ransomware no atacan a personas al azar dentro de las organizaciones, sino a empleados concretos con cargos privilegiados y funciones críticas para el negocio, a fin de aumentar sus posibilidades de afianzarse, desplazarse por la red, extraer información confidencial y monetizar el acceso.

Metodología

Durante un mes, ThreatLabz identificó a 351 víctimas comprometidas en 334 organizaciones vinculadas a un ciberdelincuente especializado en obtener acceso inicial para robar grandes cantidades de datos corporativos y cifrar de forma selectiva sistemas críticos.

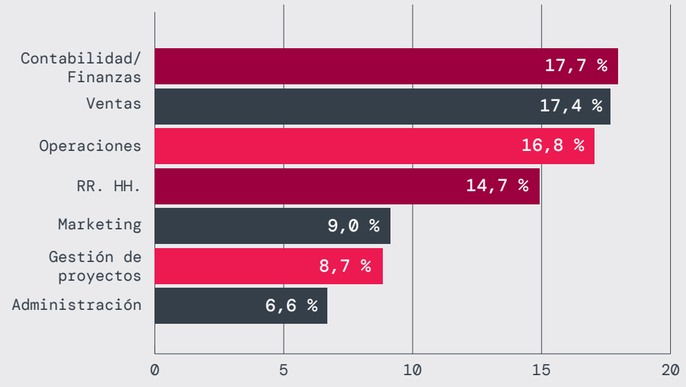


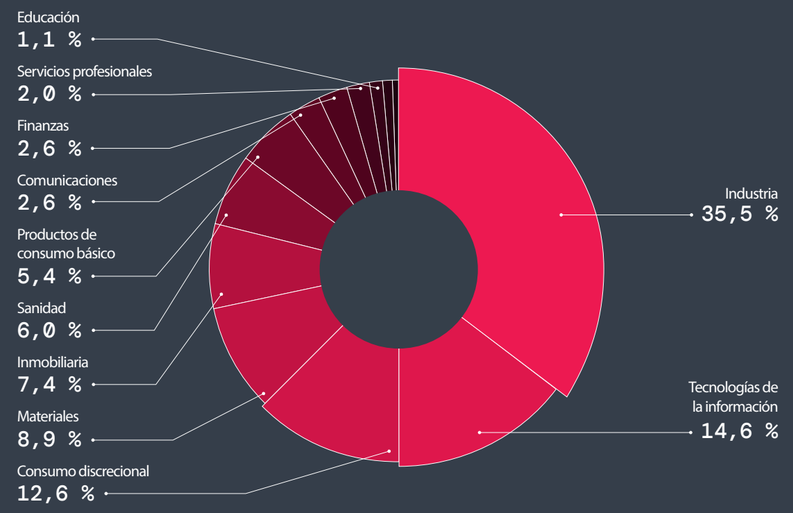
Principales conclusiones

62 % de las víctimas ocupaban un puesto directivo o superior

50 % de las víctimas trabajaban en empresas **industriales y de TI**

SE ATACARON PUESTOS CRÍTICOS PARA EL NEGOCIO





La generación X representó el **mayor porcentaje de víctimas:**

44 %

Edad media: 46
Millennials: **33 %**
Generación Z: **14 %**
Baby boomers: **9 %**

4,6 % de las empresas tenían más de un empleado comprometido

Radiografía de las víctimas de ransomware

- Las víctimas de ransomware comprometidas por este ciberdelincuente ocupaban, en su **mayoría, puestos directivos o superiores.** Esto sugiere que los atacantes se dirigen a empleados con acceso privilegiado a datos de clientes, registros financieros, contratos y sistemas operativos.
- **Más del 75 % de las víctimas pertenecían a cinco departamentos:** contabilidad/finanzas, ventas, operaciones, recursos humanos y marketing, respectivamente.
- Las víctimas abarcaban un amplio rango de edad, de los 23 a los 70 años, aunque se **concentraban entre los 45 y los 49 años; la generación X** representaba el 43,9 %.
- En cuanto a las organizaciones, el **50 % de las empresas víctimas pertenecía a solo dos sectores:** industria (35,5 %) y tecnología de la información (14,6 %).
- Más de una docena de empresas tenían **varios empleados comprometidos.**

Ejemplos de perfiles de víctimas

Estos perfiles ofrecen ejemplos reales de víctimas de ransomware y explican por qué pueden ser objeto de ataques.

Ventas regionales Responsable

Sector: Industria

Por qué es un objetivo:
acceso a cuentas de clientes, operaciones en curso, contratos, precios e información sobre ingresos

Responsable de cuentas por pagar

Sector: Tecnología de la información

Por qué es un objetivo:
acceso a datos de pago, facturas, autorizaciones financieras y registros de proveedores

Administrador de inmuebles

Sector: Inmobiliario

Por qué es un objetivo:
acceso a contratos de arrendamiento, facturas de proveedores, contratos, datos de clientes e información financiera

Responsable sénior de proyectos

Sector: Consumo discrecional

Por qué es un objetivo:
acceso a presupuestos de proyectos, contratos con proveedores y archivos o documentos confidenciales

Lección para las empresas: proteger a los usuarios empresariales de alto riesgo

Esta campaña refuerza una prioridad fundamental para la defensa frente al ransomware: fortalecer los controles en torno a los usuarios y los flujos de trabajo más próximos a los datos empresariales confidenciales. Cuando los atacantes se dirigen a empleados de ventas, finanzas, contabilidad u operaciones, una sola cuenta comprometida puede generar un riesgo para toda la empresa.

Los atacantes recurren a la urgencia, la suplantación del personal de TI y herramientas conocidas como Microsoft Teams y Quick Assist para ganarse la confianza de las víctimas. A partir de ahí, el riesgo se intensifica rápidamente y deriva en robo de credenciales, acceso remoto, desplazamiento lateral, robo de datos, posible cifrado de archivos y, en última instancia, extorsión.

La prevención del ransomware no puede limitarse a detectar el malware. También debe tener en cuenta a los empleados cuyo acceso, si se ve comprometido, genera el mayor riesgo para la empresa.

Para reducir ese riesgo, las empresas deben:

- Implementar la segmentación mediante una arquitectura de confianza cero para impedir el desplazamiento lateral y reducir la superficie de ataque.
- Formar a los empleados para que verifiquen las solicitudes del "personal de TI" mediante la información del directorio de la empresa.
- Bloquear los mensajes instantáneos y las llamadas externas en plataformas de colaboración como Microsoft Teams y Slack.
- Aplicar el principio de mínimo privilegio para limitar al máximo la exposición de sistemas y datos confidenciales.
- Implementar protección frente a amenazas en línea basada en IA y seguridad de los dispositivos para detectar y detener los ataques.
- Supervisar continuamente la actividad de usuarios, dispositivos y aplicaciones para detectar indicios de compromiso.

X **@ThreatLabz** | **Blog de investigación de seguridad** de ThreatLabz

© 2026 Zscaler, Inc. Todos los derechos reservados. Zscaler™ y otras marcas comerciales enumeradas en **zscaler.com/es/legal/trademarks** son (i) marcas comerciales registradas o marcas de servicio o (ii) marcas comerciales o marcas de servicio de Zscaler, Inc. en los Estados Unidos y/u otros países. Cualquier otra marca registrada es propiedad de sus respectivos dueños.

zscaler™ | **Act Fast. Stay Secure.**