El ransomware asciende en la estructura organizativa: los directivos son los principales objetivos

THREATLABZ RESEARCH

Los informes sobre ataques de ransomware suelen centrarse en las empresas que han sido víctimas de una violación de seguridad, los datos robados, las herramientas de malware y el pago de rescates. Sin embargo, existen muy pocos datos sobre a quiénes atacan los ciberdelincuentes dentro de las organizaciones. Un nuevo estudio de ThreatLabz cierra esta brecha y analiza el aspecto humano de los ataques de ransomware, incluyendo los puestos y las funciones empresariales más frecuentes entre las víctimas seleccionadas. Los resultados revelaron que los autores de ataques de ransomware no se limitan a atacar aleatoriamente a personas dentro de la organización, sino que se centran en empleados específicos con puestos de responsabilidad y funciones críticas para el negocio, con el fin de aumentar sus posibilidades de conseguir un punto de acceso, desplazarse por la red, sustraer información confidencial y lucrarse.

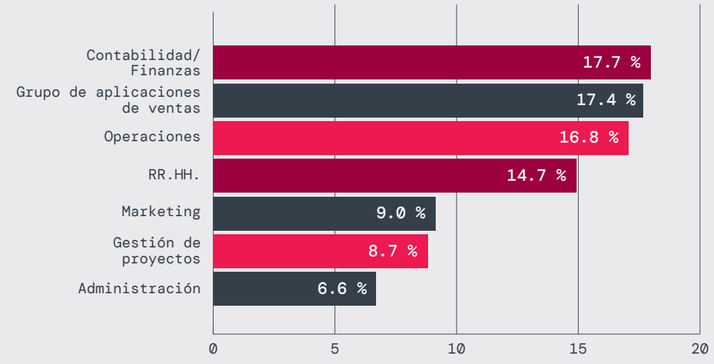
Metodología

En el transcurso de un mes, ThreatLabz identificó 351 víctimas comprometidas en 334 organizaciones vinculadas a un actor malintencionado que se especializa en obtener acceso inicial para robar grandes cantidades de datos corporativos y cifrar sistemas críticos de forma selectiva.

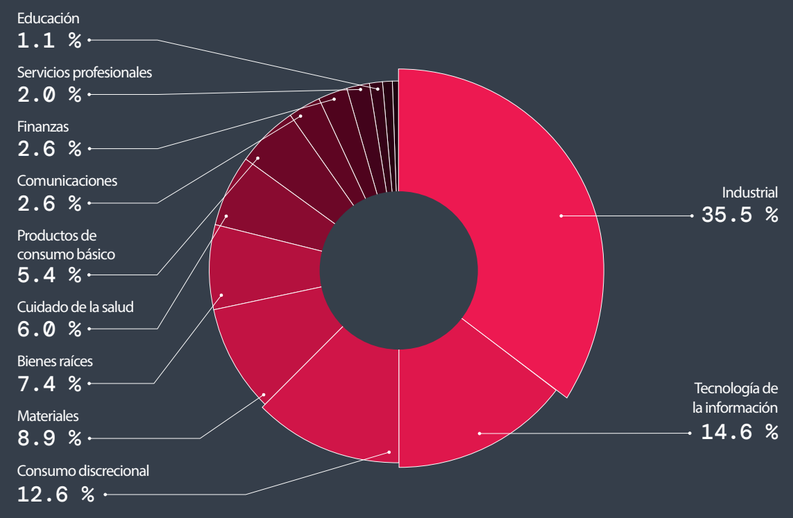
Hallazgos clave

62 % de las víctimas ocupaban un cargo de director o superior

SE SELECCIONARON LOS PUESTOS CLAVE PARA LA EMPRESA



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



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

44 %

Edad promedio: 46
Millennials: **33 %**
Gen Z: **14 %**
Baby Boomers: **9 %**

4.6 % de las empresas tenían más de un empleado comprometido

Panorama general de las víctimas del ransomware

- Las víctimas de ransomware atacadas por este grupo de ciberdelincuentes **ocupaban, en su mayoría, puestos directivos o superiores**. Esto sugiere que los atacantes atacan a empleados con acceso privilegiado a datos de clientes, registros financieros, contratos y sistemas operativos.
- El personal de **cinco departamentos representaba más del 75 % de las víctimas:** contabilidad/finanzas, ventas, operaciones, recursos humanos y marketing, respectivamente.
- Las víctimas abarcaban un espectro de edades muy amplio, desde los 23 hasta los 70 años, aunque se **concentraban en torno a los 45–50 años, y la Generación X** representaba el 43.9 % de las víctimas.
- A nivel de las organizaciones, el **50 % de las empresas afectadas procedían de tan solo dos sectores:** el industrial (35.5 %) y el de las tecnologías de la información (14.6 %).
- Varios empleados de más de una docena de **empresas se vieron afectados**

Ejemplos de perfiles de víctimas

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

Ventas regionales Director

Sector: Industriales

Por qué son objeto de ataques: el acceso a las cuentas de los clientes, las operaciones en curso, los contratos, los precios y la información sobre ingresos.

Responsable de cuentas por pagar

Sector: Tecnologías de la información

Por **qué son objeto de ataques:** acceso a datos de pago, facturas, autorizaciones financieras y registros de proveedores.

Administrador de fincas

Sector: Bienes raíces

Por qué son objeto de ataques: Acceso a contratos de arrendamiento, facturas de proveedores, contratos, datos de clientes e información financiera.

Director de proyectos sénior

Sector: Bienes de consumo discrecional

Por qué son objeto de ataques: Acceso a presupuestos de proyectos, contratos con proveedores y archivos o documentos confidenciales.

Lección empresarial: Proteger a los usuarios empresariales de alto riesgo

Esta campaña refuerza una prioridad fundamental en la defensa contra el ransomware: reforzar los controles en torno a los usuarios y los flujos de trabajo más cercanos a los datos empresariales confidenciales. Cuando los atacantes se centran en los empleados de los departamentos de ventas, finanzas, contabilidad u operaciones, una sola cuenta comprometida puede suponer un riesgo para toda la empresa.

Los atacantes recurren al sentido de urgencia, a la suplantación de identidad de profesionales de TI y a herramientas conocidas como Microsoft Teams y Quick Assist para ganarse la confianza de las víctimas. A partir de ahí, el riesgo aumenta rápidamente y puede derivar en robo de credenciales, acceso remoto, movimientos laterales, robo de datos, posible cifrado de archivos y, en última instancia, extorsión.

La prevención contra el ransomware no puede limitarse a la detección del malware. También debe tener en cuenta a los empleados cuyo acceso, en caso de verse comprometido, supone un mayor riesgo para la empresa.

Para reducir ese riesgo, las empresas deberían:

- Implementar la segmentación mediante una arquitectura Zero Trust para impedir el movimiento lateral y reducir la superficie de ataque.
- Formar a los empleados para que verifiquen las solicitudes del "personal de TI" utilizando la información que figura en el directorio de la empresa.
- Bloquear la mensajería instantánea y las llamadas externas en plataformas de colaboración como Microsoft Teams y Slack.
- Emplear el principio de acceso con privilegios mínimos para limitar al máximo la exposición a sistemas y datos confidenciales.
- Desplegar una protección contra amenazas en línea y seguridad de puntos finales basada en IA para detectar y detener ataques.
- Supervisar de forma continua la actividad de los usuarios, los dispositivos y las aplicaciones para detectar indicios de intrusión.

© 2026 Zscaler, Inc. Todos los derechos reservados. Zscaler™ y otras marcas comerciales listadas en **zscaler.com/mx/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 comercial es propiedad de sus respectivos propietarios.