LITORALPRESS

Fecha: 31-01-2025
Medio: Diario Financiero
Supl. : Diario Financiero - Inserto
Tipo: Noticia general
Título: POR QUÉ LA MINERÍA ES UN BLANCO ESTRATÉGICO PARA LOS CIBERATACANTES

Pág. : 4
Cm2: 329,2
VPE: $ 2.917.152

Tiraje: 16.150
Lectoría: 48.450
Favorabilidad: No Definida

POR QUÉ LA MINERÍA ES UN BLANCO ESTRATÉGICO PARA LOS CIBERATACANTES

Al ser una industria que incluye el trabajo de distintos actores externos y la comercialización de metales preciosos, la minería se ha convertido en un foco para los ataques informáticos. Los expertos afirman que un enfoque integral que combine tecnología, capacitación y protocolos claros, es la clave para enfrentarlos. POR SOFÍA PREUSS

La minería se convirtió en la industria que recibió, proporcionalmente, más correos electrónicos con suplantación de identidad (phishing) durante 2024 en distintos países. Así lo reveló el último reporte de la firma de seguridad de la información Hornet Security, publicación que hace énfasis en que este sector enfrenta problemas y desafíos similares a los de otros que se dedican a la fabricación, pero sobresale el hecho de que comercializa metales preciosos, factor que lo convierte en un objetivo principal para los ciberdelincuentes que buscan usar ransomware para extraer dinero de la organización.

"Considerando que en la industria existe un gran flujo de dinero, es de un gran atractivo para los atacantes solicitar un rescate económico por la información robada y/o encriptada", afirma el arquitecto de negocios estratégicos de ITQ Latam, Diego Toro.

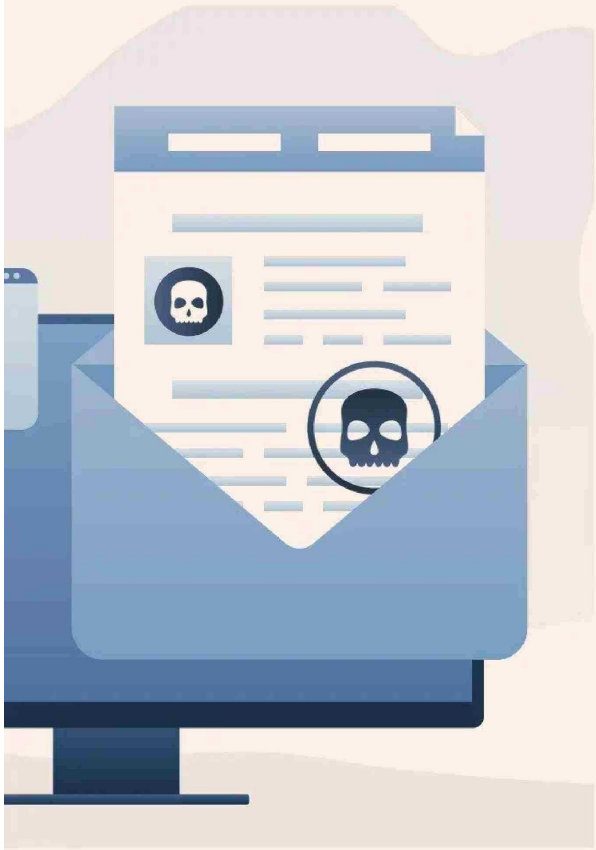
También es un blanco de este tipo de delitos porque maneja información muy relevante en cuanto a procesos, tecnología y explotaciones mineras, añade el socio de cyber en Deloitte, Marcelo Díaz. "En esa línea, los atacantes siempre intentarán enviar ataques de phishing que busquen llevar a cabo algún grado de extorsión posterior en caso de poder con-

LITORALPRESS

Fecha: 31-01-2025
Medio: Diario Financiero
Supl. : Diario Financiero - Inserto
Tipo: Noticia general
Título: POR QUÉ LA MINERÍA ES UN BLANCO ESTRATÉGICO PARA LOS CIBERATACANTES

Pág. : 5
Cm2: 498,2
VPE: $ 4.414.484

Tiraje: 16.150
Lectoría: 48.450
Favorabilidad: No Definida



Factor humano

La complejidad operativa del sector y su red de actores externos como transportistas y proveedores internacionales facilita la propagación de correos fraudulentos. "Un alto porcentaje de los colaboradores pertenecen a empresas externas, lo que dificulta tener un nivel de cobertura y seguimiento de la efectividad de las campañas", afirma el asociado de la Alianza Chilena de Ciberseguridad (ACC) y security manager de Accenture, Víctor Mitrano.

Además, en las áreas operativas y administrativas, algunos trabajadores carecen de capacitación suficiente para identificar intentos de phishing, lo que incrementa la probabilidad de que se concreten, explica el director de Ingeniería Civil Informática de la Universidad del Desarrollo (UDD), Leonardo Causa. "Este tipo de ataques no solo aprovecha las vulnerabilidades tecnológicas, sino también el factor humano, evidenciando la necesidad urgente de fortalecer tanto la infraestructura de ciberseguridad como la formación de los equipos que operan en este entorno", apunta el académico.

cultura propia en cada faena, lo cual dificulta la gestión del cambio, mientras que las tecnológicas y financieras son industrias completamente digitales o en vías de serlo", afirma.

Lo que viene

"Las amenazas están en constante evolución", afirma el socio de cyber en Deloitte, en un escenario donde la superficie de ataque sigue creciendo, las redes IoT proliferan y los espacios en cloud siguen aumentando. Con ello, la escasez de talento se ha convertido en un desafío preponderante a nivel global, indica Díaz.

El hecho de que el año pasado la minería haya sido la industria más suplantada evidencia la creciente exposición del sector frente a la digitalización de sus operaciones y la alta dependencia de cadenas de suministro globales, explica el director de Ingeniería Civil Informática de la Universidad del Desarrollo (UDD), Leonardo Causa.

"En un sector donde las operaciones dependen de sistemas industriales altamente automatizados y transacciones de gran valor, la ciberseguridad no puede ser vista como una opción, sino como una necesidad estratégica", afirma el académico. En ese sentido, apunta que las firmas deben adoptar un enfoque integral que combine tecnología, capacitación y protocolos claros, con inversión en la formación continua de los empleados, junto a la implementación de tecnologías avanzadas, como la autenticación multifactor y el cifrado de datos sensibles, apoyado con un monitoreo constante de las actividades en las redes y los sistemas. "Las empresas deben contar con un plan sólido de respuesta a incidentes que sea probado regularmente. Esto garantiza que, en caso de un ataque, las medidas correctivas puedan aplicarse de inmediato, minimizando los daños y recuperando la operación con rapidez", explica Causa.

Las medidas deben considerar tanto a la industria como sus proveedores, partiendo por la concientización de la problemática como también con políticas de exigencia y de reconocimiento para todos los entes externos, asegura el CEO de ZKTeco, Gustavo Maluenda. "El trabajo en conjunto con personal interno calificado como también con proveedores es clave para exigir estándares mínimos de exigencia y cumplimiento", ratifica.

seguir acceso a algún sistema o data específica relacionada con la explotación minera", apunta.

Distintos objetivos

A diferencia de los ataques de phishing en el sector financiero, que suelen estar dirigidos a obtener acceso a cuentas bancarias, datos de tarjetas de crédito o sistemas de pago, quienes atacan a la minería buscan credenciales para acceder a sistemas operativos, plataformas de control industrial o comunicaciones críticas relacionadas con contratos y operaciones. El asociado de la Alianza Chilena de Ciberseguridad (ACC) y security manager de Accenture, Víctor Mitrano, indica que las principales diferencias entre estos rubros es que las industrias financieras y tecnológicas vienen trabajando en generar una cultura de ciberseguridad en todos sus niveles de gestión hace muchos años, "mientras que los niveles operacionales de la minería han estado desconectados de esta temática por largo tiempo, llevando a diferenciarse en temas como la identificación de las metodologías óptimas para cada empresa y la gestión de consecuencias y escalamientos aplicables en estas".

Otro punto relevante, sostiene Mitrano, es el nivel de digitalización propio del negocio. "La minería es principalmente presencial, con trabajos en diversas ubicaciones y muchas veces con una

3%

AUMENTARON LAS MENCIONES DE CIBERSEGURIDAD EN LOS INFORMES MINEROS PRESENTADOS POR EMPRESAS GLOBALES EN EL SEGUNDO TRIMESTRE DE 2024, SEGÚN GLOBALDATA.

60%

DE LAS ORGANIZACIONES DEL SECTOR CUENTA CON PLANES CONCRETOS DE DIGITALIZACIÓN, SEGÚN EL ESTUDIO MADUREZ DIGITAL DE LA INDUSTRIA MINERA.