INFORME DE INTELIGENCIA DE AMENAZAS CIBERNETICAS

COTEDEM S.A.

Fecha de generación: 19/07/2024
Elaborado por: Jose Hernandez
Email: jhernandez@cotedem.com

Resumen Ejecutivo

Este informe proporciona una visión detallada de las amenazas cibernéticas detectadas y analizadas entre el 01/01/2024 hasta hoy. Se destacan las amenazas más críticas, los patrones emergentes y las recomendaciones para la mitigación de los riesgos. Este análisis es fundamental para fortalecer la seguridad cibernética y progteger los activos de la organización.

Gráficos obtenidos:

Detalle de Amenazas

Amenaza Crítica: Ransomware

Fuente: VirusTotal
Tipo de Amenaza: Ransomware
Nivel de Severidad: Crítica
Fecha de Detección: 2 de julio de 2024

Descripción: Se ha detectado un ataque de ransomware dirigido a varias empresas en el sector financiero. El malware cifra los archivos críticos y exige un rescate en criptomonedas para su liberación.

Acción Requerida: Implementar inmediatamente medidas de respaldo y recuperación de datos, y educar a los empleados sobre cómo reconocer y evitar correos electrónicos de phishing

---

Amenaza Alta: Phishing

Fuente: OpenCTI
Tipo de Amenaza: Phishing
Nivel de Severidad: Alta
Fecha de Detección: 10 de julio de 2024

Descripción: Se han identificado múltiples correos electrónicos de phishing que intentan engañar a los empleados para que revelen información confidencial.

Acción Requerida: Configurar filtros de correo electrónico más estrictos y realizar simulaciones de phishing para entrenar a los empleados.

Recomendaciones

1. Mejora en la Protección contra Ransomware:
- Implementar soluciones de respaldo y recuperación que sean robustas y probadas regularmente.
- Configurar sistemas de detección y respuesta ante amenazas (EDR) para identificar y bloquear actividades sospechosas.

2. Fortalecimiento de la Conciencia de Seguridad:
- Realizar capacitaciones periódicas sobre ciberseguridad para todos los empleados, enfocándose en la detección de phishing y otras técnicas de ingeniería social.
- Utilizar simulaciones de ataques para evaluar y mejorar la respuesta de los empleados ante posibles amenazas.

3. Actualización de Políticas de Seguridad:
- Revisar y actualizar las políticas de seguridad de la información para asegurar que estén alineadas con las mejores prácticas actuales y las normativas internacionales, como la ISO 27001.
- Implementar una política de contraseñas seguras y multifactor (MFA) para todas las cuentas de usuario.