CONCIBER
Comité Nacional de Seguridad Cibernética

ALERTA

Incidente Informático

Fecha: **24/10/2022**

Problemática: **Desconfiguración de Sitio Web (Defacement)**

Correlativo: **AA-0055**

Institución / Sector: **Municipalidad de San Francisco el Alto del Departamento de Totonicapán**

Nivel de priorización

Prioridad Urgente / No Urgente	Actualización Seguimiento/Preventiva/Resiliente
Urgente	**Resiliente**

Matriz de Evaluación

Riesgo Alto/ Medio/ Bajo	Nivel de Afectación		
	Integridad	Disponibilidad	Confidencialidad
Alto	**Alto**	**Alta**	**Alta**

CONTEXTO

La Municipalidad de San Francisco el Alto del Departamento de Totonicapán se vio afectada por un incidente de seguridad que afecto al sitio web institucional. El grupo de ciberdelincuentes identificado como "Negative" se atribuyó el sabotaje.

SITUACIÓN

De acuerdo a la información obtenida por el Centro Estratégico de Monitoreo – CEM, el grupo de amenazas identificado como "Negative" ejecuto el ciberataque que afecto al sitio web de la institución. No se tiene conocimiento del estado y la magnitud de la afectación, sin embargo, se pudo observar que el objetivo que buscaban los ciberdelincuentes era la desfiguración (Defacement) del sitio web institucional. La investigación refleja que la técnica empleada por los actores de amenazas es la T1491 según Mitre Attack.

RECOMENDACIONES

Considere implementar planes de recuperación ante desastres de TI que contengan procedimientos para realizar copias de seguridad de datos periódicas que se puedan usar para restaurar datos de la organización. Asegúrese de que las copias de seguridad se almacenen fuera del sistema y estén protegidas de los métodos comunes que los adversarios pueden usar para obtener acceso y destruir las copias de seguridad para evitar la recuperación

DICCIONARIO DE DATOS

- **Atacante (ciberdelincuente, actor de amenazas): Persona que realiza actividades delictivas en la red contra personas o sistemas informáticos, pudiendo provocar daños económicos o reputacionales mediante robo, filtrado de información.**
- **Defacement: técnica empleada en la desconfiguración de sitios web**

REFERENCIAS

1. **http://www.zone-h.org/archive**
2. **https://attack.mitre.org/techniques/T1491/**
3. **http://www.zone-h.org/mirror/id/40352447**

ÁREA PARA DEFINICIONES

*La información contenida en este documento y sus anexos son CONFIDENCIALES y puede contener información PRIVILEGIADA para uso exclusivo de su destinatario intencional. Si lo ha recibido por ERROR o si no es su destinatario intencional, favor NOTIFIQUELO al remitente y bórrelo inmediatamente de su sistema, así como todos los adjuntos y las COPIAS generadas. La distribución, copia u otro uso de este mensaje por terceras personas está PROHIBIDA y puede resultar ilegal.