CONCIBER
Comité Nacional de Seguridad Cibernética

ALERTA

Incidente Cibernético en la región del Caribe

Fecha: 12/04/2023

Problemática: Incidente Cibernético en República Dominicana

Correlativo: AC-0032

Institución / Sector: Instituciones Públicas y Privadas

CONTEXTO

El Instituto Agrario Dominicano de República Dominicana informo que el pasado 18 de agosto de 2022 sufrió un ciberataque de Ransomware que cifró múltiples servicios y estaciones de trabajo en toda la agencia gubernamental.

SITUACIÓN

detrás del ataque cibernético que comprometió múltiples servicios y estaciones de trabajo del Instituto Agrario Dominicano se encuentra "QUANTUM RANSOMWARE". Esta amenaza de tipo malware afectó bases de datos, aplicaciones, correos electrónicos e incluso cifro información de la institución. Hasta el momento no se tiene el dato exacto de la cantidad y que tipo de información fue exfiltrada por los Ciberdelincuentes.

Nivel de priorización

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

Matriz de Evaluación

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

RECOMENDACIONES

Considere implementar:

- Servicios de Antivirus/Antimalware.
- Herramientas de Prevención de Intrusiones en la red (IDS)
- Herramientas de Detección y Respuesta de Amenazas de Puntos Finales (EDR)
- Herramientas de Detección y Respuesta Extendidas (XDR)

Es importante:

- Actualizar regularmente los sistemas operativos, el hardware y el software de los dispositivos.
- Llevar a cabo una rutina periódica de actualización y parcheo de los sistemas operativos y programas ofimáticos.
- Implementar planes de recuperación ante desastres de TI que contengan procedimientos para realizar y probar regularmente copias de seguridad de datos que se pueden usar para restaurar datos de la organización.

DICCIONARIO DE DATOS

1. Endpoint Detection and Response-EDR (Detección y Respuesta de Amenazas de Puntos Finales): Tecnología de ciberseguridad que monitorea continuamente un "punto final" para mitigar amenazas cibernéticas maliciosas
2. Extended Detection and Response - XDR (Detección y Respuesta Extendidas): Tecnología de ciberseguridad que monitorea y mitiga las amenazas de ciberseguridad
3. Ciberdelincuente: Persona que se aprovecha de fallas de seguridad encontradas en plataformas, programas o sistemas a título personal
4. Cifrado: Operación o función matemática utilizada en combinación con una clave que se aplica a un texto en claro y permite obtener un texto cifrado (o descifrarlo) garantizando la confidencialidad e integridad de la información contenida.
5. Malware: Es un programa malicioso que tiene como característica principal su alto grado de dispersabilidad, es decir, lo rápidamente que se propaga.
6. Ransomware: Es un tipo de malware que impide y/o secuestra el acceso a archivos del sistema infectado, en ocasiones cifrándolos, y coacciona al usuario para pagar un rescate a cambio de su liberación.

REFERENCIAS

1. https://cncs.gob.do/centro-de-ciberseguridad-trabaja-junto-al-iad-para-restaurar-servicios-y-reducir-el-impacto-frente-a-incidente-cibernetico/#:~:text=El%20Centro%20Nacional%20de%20Ciberseguridad,contempla%20el%20pago%20de%20recompensas.
2. https://devel.group/ataque-de-quantum-ransomware-en-republica-dominicana/
3. https://github.com/develgroup/SOC_IOCs/tree/main/20220506_02_QuantumRansomware