

Ushuaia, 15 de Julio de 2024

Letra: S.S.D.A.I.T.d.F.A.I.A.S.

Cde. Expte: E-59148-2024

# Informe Ciberataque Domingo 23 de Junio 2024

## Secretaría de Servicios Digitales

### Introducción

Este informe técnico tiene como objetivo documentar el ciberataque sufrido por la infraestructura tecnológica del Gobierno provincial el domingo 23 de Junio de 2024 alrededor de las las 3:40 a.m. El propósito de este documento es proporcionar detalles técnicos que sirvan a los diversos procedimientos administrativos/legales correspondientes.

### Descripción del Incidente

El día domingo alrededor de las 3:40 a.m., la infraestructura tecnológica del Gobierno provincial fue objeto de un ciberataque que comprometió múltiples sistemas críticos. El Vector de ingreso esta siendo investigado por el equipo técnico de la Agencia de innovación junto a un equipo de respuesta a incidentes y ciberseguridad En un principio se identificaron un numero de credenciales robadas pertenecientes a los dominios: TDF.gob.ar y Tierradelfuego.gob.ar, entre otras. Se sospecha que dichas credenciales fueron utilizadas por los autores del ransomware como vector de entrada a la red de datos del gobierno provincial.

### Propagación del Malware

El malware, aparentemente una variante de ransomware dirigida específicamente a productos de virtualización, posiblemente utilizó técnicas de movimiento lateral para propagarse por la red interna, afectando principalmente los datastores (unidades de almacenamiento) de la infraestructura de virtualización basada en VMware y comprometiendo las copias de seguridad almacenadas.

## Impacto en los Sistemas

El ciberataque comprometió los siguientes componentes críticos:

### *Infraestructura de Virtualización (VMware)*

El malware posiblemente se propagó a través de los hipervisores y luego hacia los datastores virtuales, comprometiendo la integridad y disponibilidad de los sistemas alojados localmente y sus respaldos de seguridad. Se observaron comportamientos característicos de técnicas de lateral movement, lo que aparentemente permitió al malware acceder y corromper múltiples sistemas dentro de la red de virtualización.

### *Detalles Técnicos*

- **Vectores de Infección:** Los datastores virtuales fueron comprometidos mediante la explotación de vulnerabilidades en los servicios de gestión de VMware.
- **Impacto en Sistemas:** La corrupción de los datastores resultó en la indisponibilidad de varios sistemas críticos, interrumpiendo servicios esenciales.

### *Copias de Seguridad*

Las copias de seguridad, fueron parcialmente comprometidas por la infección, impidiendo la restauración inmediata de los sistemas afectados. El análisis inicial indica que el malware habría ejecutado procesos de cifrado utilizando algoritmos de criptografía, haciendo que los datos sean inaccesibles sin la clave de descifrado.

### *Detalles Técnicos*

- **Métodos de Compromiso:** El malware habría accedido a las copias de seguridad a través de credenciales robadas y posibles vulnerabilidades de software.
- **Técnicas de Cifrado:** probablemente se hizo uso de algoritmos de cifrado asimétrico dificultando la recuperación de los datos sin la clave de descifrado.
- **Evaluación de Daños:** Se continúa analizando de manera la implicancia del daño realizado a la información almacenada, en permanente contacto con las áreas afectadas.

## **Medidas Inmediatas Tomadas**

Desde la mañana del domingo, el equipo técnico de la Secretaría de Servicios Digitales ha implementado una serie de medidas de contención y recuperación:

- **Segmentación de Red:** Implementación de políticas de segmentación de red para contener la propagación del malware y mantener aisladas las redes críticas.
- **Creación de Entornos Seguros:** Establecimiento de entornos aislados (sandboxing) para la recuperación y análisis de sistemas afectados.

## *Restauración de Servicios Críticos*

El equipo técnico trabajó en la restauración de los servicios críticos necesarios para mantener la operatividad del Gobierno provincial. La prioridad se centró en recuperar los sistemas esenciales para las operaciones diarias, incluyendo sistemas de gestión administrativa, liquidación de haberes, servicios de atención al ciudadano y plataformas de comunicación interna.

## *Detalles Técnicos*

- **Recuperación de Sistemas:** Uso de imágenes limpias y respaldos no comprometidos para la restauración de sistemas críticos.
- **Servicios Esenciales:** Priorización de sistemas esenciales mediante un enfoque de recuperación gradual y por etapas.

## *Evaluación de Daños y Pérdida de Información*

Se lleva a cabo una evaluación continua de los daños y la pérdida de información junto a un equipo externo de respuesta de incidentes y ciberseguridad. Esto incluye la revisión exhaustiva de los sistemas comprometidos, la identificación de datos perdidos o dañados, y la implementación de medidas de seguridad adicionales para prevenir futuros ataques.

## *Evaluación inicial de Daños*

La evaluación inicial ha identificado los siguientes daños:

### *Compromiso*

Se ha constatado el compromiso de datos almacenados en la infraestructura de virtualización y en las copias de seguridad. La evaluación de este aspecto continúa mientras se avanza en las tareas de recuperación.

Varios servicios alojados localmente han sido interrumpidos, afectando las operaciones en diversas áreas del Gobierno provincial. Los sistemas comprometidos incluyen:

#### **1. Controladores de dominio, DHCP, DNS**

- Servidores de núcleo que garantizan el funcionamiento de la red de datos y la validación de usuarios. Este servicio se encuentra operando nuevamente.

#### **2. Controladores de activos de red**

- Plataforma utilizada para la gestión de activos de red y su correspondiente monitoreo.

#### **3. Sistemas de Cargas de Horas de Guardias:**

- Gestión de horarios y turnos del personal de guardia en diferentes áreas administrativas y de emergencia.

#### **4. Liquidador de Haberes y Subsidios:**

- Procesamiento de salarios, bonificaciones y subsidios para empleados públicos y beneficiarios de programas sociales.

#### **5. Liquidación de Subsidios:**

- Administración y distribución de subsidios para sectores específicos como salud, educación y desarrollo social.

#### **6. Control de Cargas de Gas Licuado de Petróleo (GLP):**

- Supervisión y regulación de la distribución y utilización de las asistencias económicas para la carga de gas licuado de petróleo en la provincia.

#### **7. Sistemas de Trámites de Exportación de Industria:**

- Gestión y seguimiento de trámites relacionados con la exportación de productos locales, incluyendo permisos y documentación aduanera. Actualmente este sistema no se encuentra disponible y se encuentra seriamente comprometido para su recuperación. Se ha puesto en conocimiento al área usuaria de este sistema y se están tomando medidas de contingencia para evitar la demora en estos trámites a los usuarios.

#### **8. Sistema de Correo Electrónico:**

- Comunicaciones internas y externas a través de plataformas de correo electrónico institucionales. Se han generado cuentas de contingencia por cada Ministerio para garantizar la comunicación por esta vía.

## 9. Sitios Institucionales:

- Portales web oficiales del gobierno provincial utilizados para la difusión de información, servicios y contacto con la ciudadanía.

### 10. **Plataformas Virtuales de Educación:**

- Campus de establecimientos educativos provinciales, utilizado por alumnos y docentes.

### 11. **Novedades de cargas de novedades Docentes (SIGE):**

- Información relevante y cursos específicos dirigidos al cuerpo docente y administrativo del sistema educativo provincial.

### 12. **Sitio de autoconsulta de recibos de haberes**

- Portal de auto consulta de los recibos de haberes. Actualmente el equipo de sistemas se encuentra restableciendo este servicio para tenerlo operativo a la brevedad.

### 13. **Plataforma de Capacitación Interna - IPAP:**

- Espacio digital para la capacitación continua y el desarrollo profesional de los empleados públicos en diferentes disciplinas.

### 14. **Servidor de Archivos:**

- Repositorio de información utilizado de manera interna.

### 15. **Gestión Interna (SIGA):**

- Sistema de gestión de trámites administrativos/contables.

### 16. **Sistemas de Gestión de Trámites a Vecinos:**

- Plataformas digitales para la realización y seguimiento de trámites administrativos y servicios públicos ofrecidos a los ciudadanos.

### 17. **Sistema de Gestión de documentos – Registro Civil (GDE)**

- Plataforma de gestión digital de trámites y manejo de documentos.

Este listado y enumeración de sistemas se encuentra en permanente estado de evaluación y actualización trabajando en conjunto a las áreas afectadas.

**Estado Actual:** Se está realizando una evaluación continua de los daños y la pérdida de información. Esto incluye la revisión de los sistemas comprometidos, la identificación de datos perdidos o dañados, y la implementación de medidas de seguridad adicionales para prevenir futuros ataques, como así también la coordinación de medidas de contingencia ante la falta de sistemas para no afectar la continuidad de las operaciones administrativas diarias.

**Acciones Adicionales en Curso:** Actualmente, se continúa trabajando de manera intensiva con el fin de lograr la completa recuperación de los sistemas afectados. Se están ejecutando las siguientes acciones:

- **Comité de Emergencia Técnica Interdisciplinario:** Se ha conformado un comité de emergencia técnica interdisciplinario con expertos en ciberseguridad y tecnología de la información para coordinar las acciones de análisis, protección y mitigación de riesgos.
- **Correcciones Técnicas:** El equipo técnico de la Secretaría de Servicios Digitales, de la Agencia de Innovación, está implementando correcciones y mejoras en los sistemas de seguridad.

### **Conclusión:**

El ciberataque ha tenido un impacto significativo en la infraestructura tecnológica del Gobierno provincial, afectando la disponibilidad de servicios críticos y resultando en la pérdida de datos. Sin embargo, se han tomado medidas inmediatas para aislar la infección y comenzar la recuperación de los sistemas afectados. El equipo técnico continúa trabajando para restaurar completamente los servicios y asegurar que se implementen medidas de prevención efectivas para evitar futuros ataques. Se está fortaleciendo la seguridad con expertos en la temática y estableciendo un sistema de contingencia ante cualquier nuevo ataque. Se comunicará progresivamente a las áreas correspondientes la restauración de los sistemas que les afecten.

Lic. Calderini Matias  
Secretaría de Servicios Digitales

Agencia de Innovación de Tierra del Fuego AIAS

Firmado Electrónicamente por  
LICENCIADO/A CALDERINI MATIAS EZEQUIEL  
Gobierno de Tierra del Fuego  
SECRETARIO DE SERVICIOS DIGITALES  
16/07/2024 15:57