Informe ciberataque JPMP

Responder | Responder a todos | Reenviar

HV

Henry Vargas Sierra

Para 'luz.correa@fac.mil.co'; TC. Luz Esperanza Correa Cruz; Mauricio Andres Tellez Garces

CC Sandra Patricia Mejia Garatejo; Helman Rene Jaramillo Valderrama; Oscar Leonardo Perez Casilimas

lunes 21/07/2025 10:17 a. m.

Mensaje reenviado el 25/07/2025 11:34 a. m..

InsightsReport-Posture-CampaignEvents-PrevalentCampaigns_1752870020780.pdf
42 KB

Trellix_insights_security_brief_1752870132081.pdf
433 KB

FORMATO REGISTRO INCIDENTES.pdf
508 KB

Buenos días,

Cordial saludo, de acuerdo con nuestra última reunión donde se expuso por parte de la Justicia Penal Militar y Policial, el tema del ciberataque del cual fuimos victimas en el pasado mes de junio, atentamente me permito remitir el informe con el detalle de lo sucedido al igual las acciones para mitigación y recuperación de la operación, al igual reportes generados en la herramienta Trellix Insights donde se evidencia una puntuación para las categorías de Gestión de contenido, Protección de día cero, Problemas de configuración y Elementos de seguridad positivos, las cuales entre mayor sea su puntuación es debido a que el control esta activo y funcionando correctamente, por otra parte, se muestra información sobre campañas de ataques asociadas que se han presentado últimamente y si alguna de ellas se ha presentado en la entidad, al igual algunas recomendaciones.

Agradezco su atención y quedo atento a cualquier inquietud.

Atentamente,

HENRY VARGAS SIERRA
Jefe Oficina TIC
Henry.vargas@justiciamilitar.gov.co
Teléfono: (+57) (601) 5169563 Ext. 1480
Cra. 46 No. 20C 01 Cantón Militar Occidental
"Coronel Francisco José de Caldas"
Bogotá
www.justiciamilitar.gov.co

Fecha Diligenciamiento: 17/07/2025

FORMATO REGISTRO INCIDENTES
ALERTA: RANSOMWARE FOG
Clasificación: Crítica

Información General del Incidente

- **Fecha y hora de detección:** 15/06/2025.
- **Fecha y hora de inicio (si se conoce):**
- **Entidad afectada:** Unidad Administrativa Especial de Justicia Penal Militar y Policial.
- **Persona/Área responsable de la notificación:** Henry Vargas Sierra – Jefe Oficina de Tecnologias de la Información y las Comunicaciones.

Descripción del Incidente

- **Tipo de incidente:** Ransomware.
- **Descripción breve:** El Ciber Ataque del que fue objeto la Unidad Administrativa Especial de Justicia Penal Militar y Policial, corresponde a la naturaleza de intrusión por Ransomware Gunra, el cual es una variante de malware (software malicioso) reciente, identificado en abril de 2025, que representa una amenaza de alta categoría, para organizaciones y empresas, a nivel global. El ataque se dirige, principalmente, a sistemas Windows. Este Ransomware se ha empleado como instrumento de ataque en diversas industrias, incluyendo sectores de bienes raíces, farmacéutica y manufactura, así como instituciones de salud y gubernamentales, en distintos países
- **Impacto:** Interrupción del funcionamiento y atención de la Unidad Administrativa Especial de Justicia Penal Militar y Policial dado que se afectó el Tenant de Microsoft365 y los nodos de infraestructura tecnológica (hiperconvergencia).
- **Gravedad o nivel de criticidad:** Crítico.

Cronología (Timeline)

Línea de tiempo detallada: Eventos clave en orden cronológico (detección inicial, contención, escalamiento, recuperación, cierre).

- **15/06/2025**
    - 05:00 – Se detecta el cifrado de los nodos de hiperconvergencia
    - 05:30 – Se notifica al área de TI.
    - 06:00 – Se realiza la contención

- 07:00 – Primer informe del resultado de la inspección de los daños causados por el ransomeware.
- 09:00 Mesa técnica para evaluar la magnitud del ataque
- 10:00 Comunicación con el director de la UAE-JPMP informando la situación del ataque
- 10:15 Comunicación con el CSIRT informando la situación del ataque
- 14:00 – Segundo informe del resultado de la inspección de los daños causados por el ransomeware.
- 18:00 – Informe final del resultado de la inspección de los daños causados por el ransomeware.

- **16/06/2025 al 09/07/2025**
  - Recuperación de la operación de la Unidad Administrativa de Justicia Penal Militar y Policial

Análisis de Causa Raíz

- **Vulnerabilidades o brechas de seguridad explotadas:**
  - Configuraciones débiles,
  - Credenciales comprometidas
  - Credenciales débiles
- **Vector de ataque principal:**
  Phishing (correo malicioso)
- **Factores contribuyentes (indirectos):**
  - Falta de concientización del personal
  - Privilegios excesivos.

Indicadores de Compromiso (IoCs)

- **Firma o nombre del ransomware (si se conoce):**
  - Ransomeware Gunra de abril 2025

Medidas de Contención y Erradicación

- **Acciones tomadas para contener el incidente:**
  - Aislamiento de equipos infectados
  - Desconexión de la red
  - Bloqueos de puertos
- **Herramientas utilizadas:**

- Software antivirus,
- EDR
- NX sistemas de monitoreo de red
- Análisis forense

- **Tiempos de respuesta:**
  El problema se aislo en una hora
  EL RTO fue de 2.5 semanas.
- **Descripción del proceso de recuperación:**
  Restauración desde respaldos (backups), reconstrucción de sistemas, verificación de la integridad de los datos, etc.

Impacto Detallado

- **Sistemas comprometidos:**
  - Infraestructura de hiperconvergencia
  - Conectividad a nivel local y nacional
  - Tenant de Microsoft 365
  - Operación a nivel local y nacional
- **Datos comprometidos o cifrados:**
  - Tenant de Microsoft 365
    - SharePoint
    - One Drive
- **Afectación a la operación:**
  - El tiempo de inactividad fue de 2.5 semanas
  - Se comprometieron todos los procesos de la Unidad Administrativa Especial de Justicia Penal Militar y Policial
  - Daños a la reputación dado que en medios nacionales y canales de youtube se propagaron noticias falsas lo cual afectó la reputación.
- **Requerimiento de rescate y situación de pago:**
  - Existió una demanda monetaria por parte del atacante quien dejo un archivo R3adm3.txt con las instrucciones, por parte de la Unidad Administrativa Especial de Justicia Penal Militar y Policial ninguna persona realizó alguna negociación, por ende, no se realizó ningún pago.

Plan de Recuperación y Validación

- **Plan de restauración:**
  - Reinstalación desde cero de la plataforma de hiperconvergencia
  - Restauración tenant Microsoft 365
  - Fortalecimiento en la plataforma de antivirus, instalación EDR y NDR
  - Fortalecimiento en seguridad perimetral
- **Validación de la integridad de la restauración:**

Se realiza constate monitoreo de alertas y logs a través de la plataforma de trellix con EDR y NDR

- **Tiempos y costos de la recuperación:**

Los costos asociados a este ataque fueron de cinco mil millones de pesos.

Acciones Correctivas y Preventivas

Para la Justicia Penal Militar y Policial, resulta imperativo adoptar un enfoque integral de ciberseguridad y continuidad de negocio, alineado con los estándares internacionales (como ISO/IEC 27001 y NIST SP 800-53), que fortalezca las capacidades de protección, detección, respuesta y recuperación frente a amenazas cibernéticas. Este enfoque contempla la gestión sistemática de vulnerabilidades a través de ciclos programados de patch management, la reconfiguración avanzada de dispositivos perimetrales (firewalls de próxima generación, IPS/IDS) y el endurecimiento de sistemas mediante políticas robustas de autenticación multifactor (MFA), controles de acceso basados en roles (RBAC) y gestión segura de credenciales, garantizando la integridad, confidencialidad y disponibilidad de la información judicial y procesal.

Por otro lado, y no menos importante la segmentación lógica de redes mediante VLANs y microsegmentación con políticas Zero Trust, limitará la superficie de ataque y contendrá posibles intrusiones, protegiendo especialmente los activos de alto valor y la información clasificada. De forma complementaria, se fortalecerán los procesos de concienciación mediante programas de capacitación en seguridad de la información dirigidos a todos los niveles del personal —desde operadores judiciales hasta personal técnico—, incluyendo simulaciones de ataques tipo phishing, formación en manejo seguro de evidencias digitales y cumplimiento normativo en protección de datos.

Lecciones Aprendidas Especificas

- Fortalecimiento de defensa cibernéticas robustas ya avanzadas
- Importancia en la segmentación de la red (VLans) y gestión de privilegios
- Identificación a respuestas rápida a incidentes
- Verificación constante de activos críticos
- Escaneo exhaustivo y reincorporación controlada de equipos
- Colaboración con soporte técnico especializado
- Determinación de un punto de recuperación óptimo
- Participación en comités de seguridad digital

Documentación y Evidencias

- Se radicó una denuncia formal ante la Policía Judicial (DIJIN), identificada con el número de noticia criminal 110016099382202500021. Este proceso, iniciado por el Fiscal URI número 12, avanzó el 18 de junio de 2025, cuando la Justicia Penal Militar y Policial suministró la evidencia: los logs de los visores de hiperconvergencia. Además, se obtuvieron los registros detallados de un equipo de usuario y de los equipos de seguridad perimetral (firewall), abarcando el periodo del 12 al 16 de junio de 2025. Toda esta información crítica fue entregada y asegurada en un medio de almacenamiento digital

- Se inició el proceso de afectación de la póliza de Responsabilidad Civil número 1009120 de Previsora Seguros, contratada por la Unidad Administrativa Especial de la Justicia Penal Militar. Esta póliza tiene la cobertura de Responsabilidad por seguridad de datos. La reclamación ha sido registrada formalmente ante la aseguradora bajo el número 20251806.

- El 24 de junio de 2025, la Justicia Penal Militar y Policial (JPMP) participó activamente en la sesión extraordinaria del Comité Nacional de Seguridad Digital. Esta reunión, liderada por el doctor Saúl Kattan Cohen, alto consultor presidencial para la Transformación Digital, se convocó con el propósito fundamental de abordar en detalle el reciente ciberataque que impactó a la Entidad. Durante la sesión, la Justicia Penal Militar y Policial tuvo la oportunidad de exponer pormenorizadamente los hechos y el contexto de lo sucedido, por otra parte, el doctor Kattan no solo proporcionó una visión estratégica, sino que también ofreció un conjunto de recomendaciones y directrices cruciales destinadas a fortalecer de manera integral las capacidades de ciberseguridad dentro de la Justicia Penal Militar y Policial. Estas directrices son vitales para blindar los sistemas y la información frente a futuras amenazas digitales.

Datos del Contacto Clave

- **Equipo interno de respuesta:**
  - Helman René Jaramillo
    Coordinador de grupo de infraestructura
    Helman.jaramillo@justiciamilitar.gov.co
  - Oscar Leonardo Perez
    Coordinador de grupo de redes y comunicaciones
    oscar.perez@justiciamilitar.gov.co

- Henry Vargas S.
  Jefe de oficina de TIC
  Henry.vargas@justiciamilitar.gov.co