En las últimas semanas, se han registrado varios ataques informáticos dirigidos a entidades estatales en Colombia, afectando de manera significativa la operación y la seguridad de la información institucional. Tras investigaciones realizadas por el CISRT Salud, se ha identificado que un patrón común en estos incidentes es la utilización del ransomware **GUNRA** por parte de los actores de amenaza involucrados.

Entidades estatales comprometidas

Desde del CSIRT Salud se ha constatado con el uso de fuentes externas, que a nivel nacional se han presentado en lo corrido de junio de 2025 los siguientes ataques a entidades del orden gubernamental:

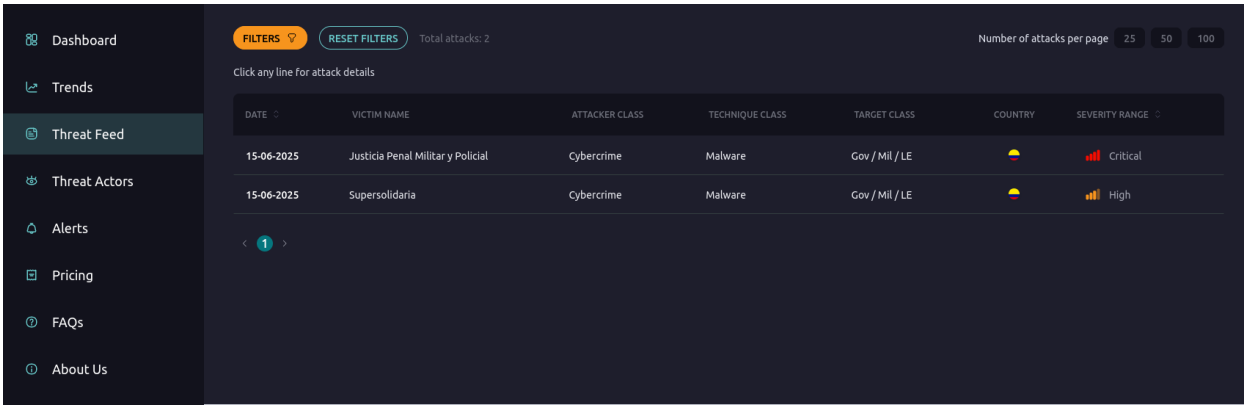

Imagen tomada de herramienta de verificación

Tras verificar cada uno de estos incidentes de seguridad, se ha detectado el uso de técnicas y tácticas similares asociadas al uso del ransomware GUNRA, tal como se evidencia a continuación:

CSIRTSALUD-AL-20250618-005

TLP: CLEAR

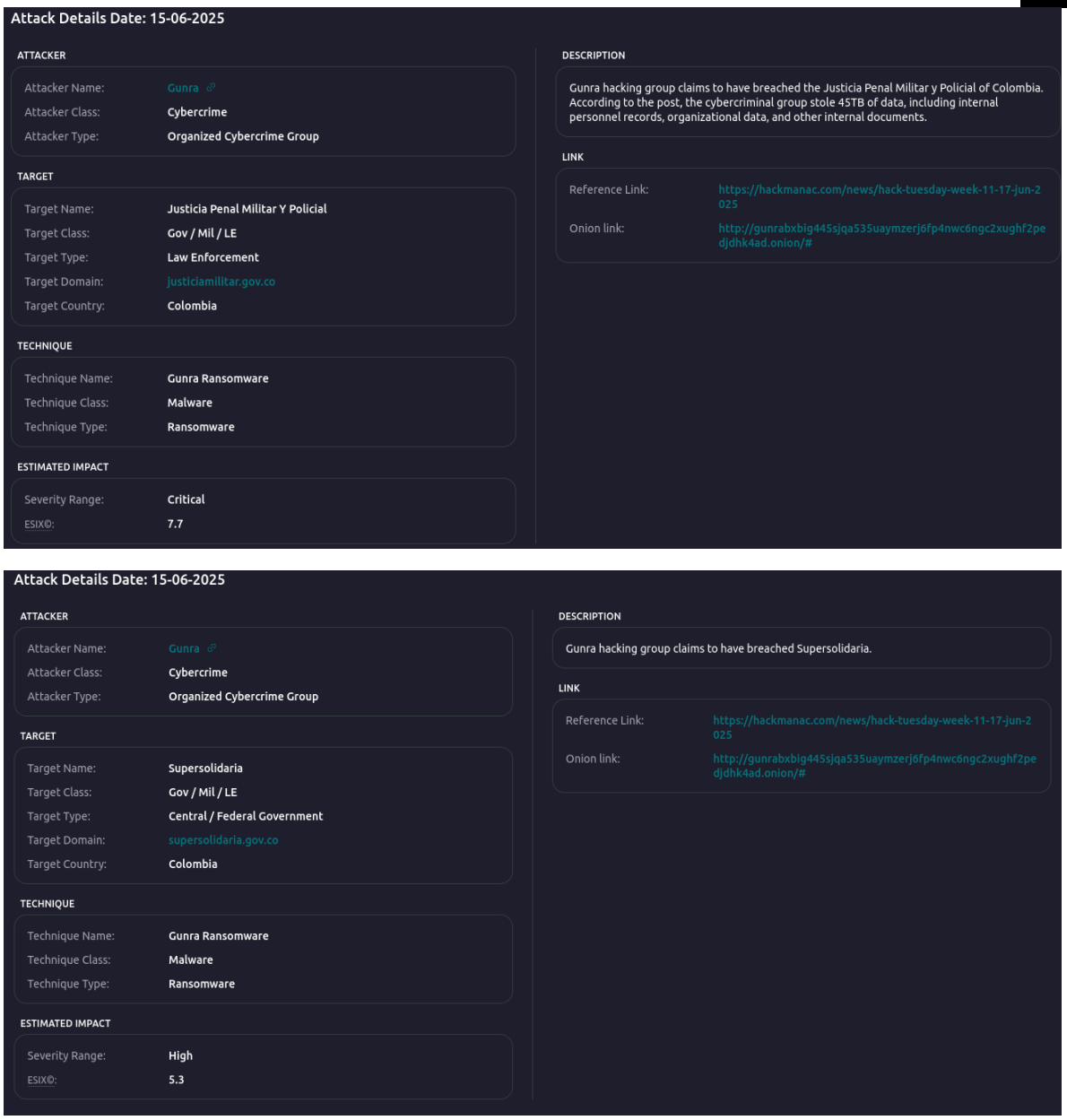

Imagen tomada de herramienta de verificación

¿Qué es el Ransomware GUNRA?

Gunra Ransomware es un tipo de software malicioso diseñado para cifrar datos digitales y exigir el pago de un rescate para restaurar el acceso. Este ransomware añade la extensión de

archivo **.ENCRT** a cada archivo cifrado, transformando los nombres de archivo como document.docx a document.docx.ENCRT, impidiendo así que los usuarios accedan a sus propios datos. El ransomware emplea sofisticados algoritmos de cifrado, lo que hace prácticamente imposible el descifrado sin las claves necesarias. Una vez que el ransomware completa el proceso de cifrado, crea una nota, la **R3ADM3.txt**, que suele colocarse en los directorios afectados y se muestra de forma destacada en el escritorio de la víctima. Esta nota de rescate explica el problema del cifrado, denuncia el robo de datos empresariales confidenciales y describe el proceso de contactar a los ciberdelincuentes a través de la red Tor para, potencialmente, recuperar el acceso a los archivos comprometidos. Las víctimas suelen ser inducidas a contactar a los atacantes con el incentivo de descifrar algunos archivos gratuitamente como prueba de su capacidad, junto con una severa advertencia de que los retrasos o la falta de cooperación provocarán la exposición de datos públicos.

En la imagen relacionada a continuación se muestra un ejemplo del archivo .txt en la que los atacantes notifican el cifrado de la información y la solicitud del pago del rescate.

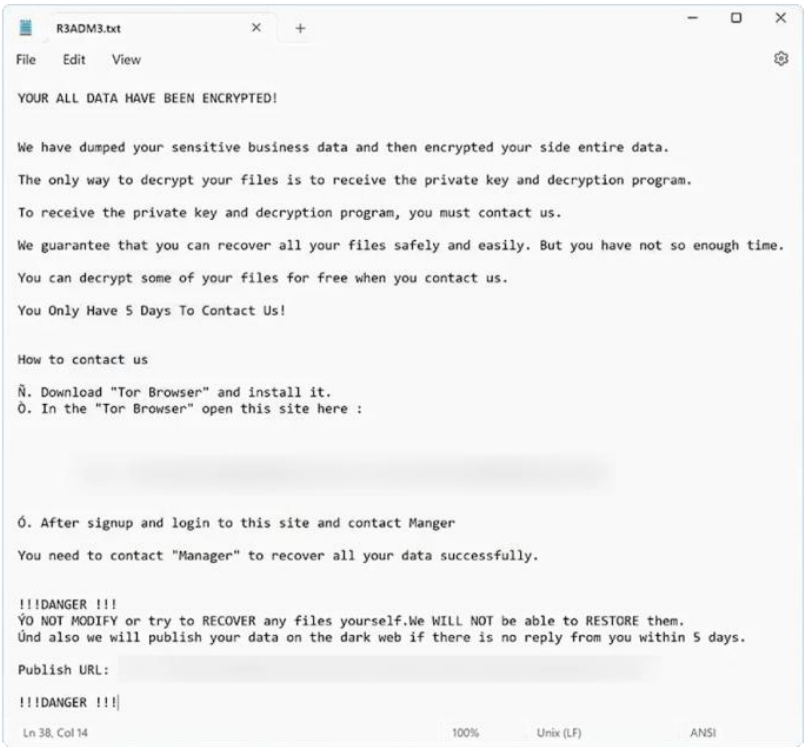

Imagen tomada de bugsfighter.com

Impacto y riesgos:

Impacto principal	Riesgo asociado
Interrupción de servicios críticos	Pérdida de información y continuidad operativa
Cifrado y secuestro de datos	Exposición de datos sensibles y sanciones
Robo y filtración de información	Daños reputacional y pérdida de confianza
Costos económicos elevados	Incentivo a nuevos ataques y extorsión

El *Ransomware* GUNRA representa una amenaza grave y multifacética para las entidades estatales y del sector salud, con impactos que van desde la interrupción de servicios esenciales hasta la exposición de datos sensibles y la pérdida de confianza institucional

Indicadores de Compromiso:

GUNRA es una variante de ransomware derivada de Conti, escrita en C/C++, que se caracteriza por filtrar información confidencial antes de cifrar los archivos de la víctima y exigir un rescate. A continuación se detallan los principales indicadores de compromiso (IoC) asociados a esta amenaza, útiles para la detección y respuesta:

- **Extensión de archivos cifrados**: Los archivos afectados reciben la extensión .ENCRT (por ejemplo, documento.docx.ENCRT)
- **Nota de rescate:** Se crea un archivo llamado R3ADM3.txt en los directorios afectados, con instrucciones para contactar a los atacantes a través de un sitio .onion en la red Tor y un plazo de cinco días antes de la publicación de los datos robados
- **Hashes de archivos maliciosos conocidos:**
  - MD5: 9a7c0adedc4c68760e49274700218507

- SHA-256: 854e5f77f788bbbe6e224195e115c749172cd12302afca370d4f9e3d53d005fd

- **Técnicas y tácticas observadas**:
  - Eliminación de copias de seguridad y shadow copies mediante WMI para imposibilitar la restauración del sistema2.
  - Enumeración de procesos y recopilación de información del sistema tras la infección.
  - Uso de técnicas de evasión y antianálisis, incluyendo la ofuscación y la evasión de sistemas de detección basados en reglas2.
  - Comunicación con infraestructura de mando y control (C2) a través de proxies (MITRE ATT&CK T1090)2.
  - Cifrado de datos como principal impacto (MITRE ATT&CK T1486)

Estos IoC deben integrarse en sistemas SIEM, EDR y herramientas de inteligencia de amenazas para una detección y respuesta proactiva frente a GUNRA y variantes relacionadas.

Cómo se realiza la infección:

El ransomware Gunra se infiltra en los ordenadores principalmente mediante tácticas de phishing e ingeniería social. Los ciberdelincuentes suelen camuflar archivos maliciosos como adjuntos legítimos o incluirlos en software aparentemente inofensivo, incitando a los usuarios a descargarlos y abrirlos. Estos archivos infecciosos pueden adoptar diversos formatos, como archivos ZIP, archivos ejecutables o documentos con macros maliciosas. Una vez ejecutado, el ransomware Gunra puede cifrar rápidamente los archivos del sistema, añadiendo la extensión ".ENCRT" a cada archivo afectado. Además, este ransomware puede propagarse a través de vulnerabilidades de red o autopropagarse a través de dispositivos de almacenamiento extraíbles. Para mitigar el riesgo de infección, se recomienda a los usuarios **tener cuidado con los correos electrónicos no solicitados**, evitar la descarga de software de fuentes no verificadas y mantener una protección antivirus robusta.

Recomendaciones:

Para las entidades del sector salud que forman parte del ecosistema digital, es fundamental adoptar las siguientes medidas preventivas para evitar la materialización de esta amenaza en su infraestructura tecnológica:

Recomendaciones	Detalle
	**1. Fortalecimiento en la capacitación**: • Capacitar al personal sobre la identificación de correos sospechosos y buenas prácticas de seguridad digital • Restringir el uso de dispositivos extraíbles y limitar privilegios de usuario. **2. Actualización y Parcheo** • Mantener actualizados los sistemas operativos, aplicaciones y dispositivos de red, aplicando los parches de seguridad recomendados por los fabricantes. **3. Copias de Seguridad** • Realizar respaldos periódicos de la información crítica y almacenarlos en ubicaciones seguras, desconectadas de la red principal. **4. Monitoreo y Detección** • Implementar soluciones de monitoreo continuo y detección de amenazas (SIEM, EDR) para identificar comportamientos anómalos y responder oportunamente. **5. Segmentación de Red** • Separar las redes administrativas, clínicas y de usuarios para limitar la propagación del ransomware en caso de infección. **6. Plan de Respuesta a Incidentes** • Desarrollar y probar planes de respuesta ante incidentes, incluyendo procedimientos específicos para ataques de ransomware. **7. Recomendaciones Adicionales**

Recomendaciones	Detalle
	• Revisar y reforzar las políticas de acceso remoto y autenticación multifactor. • Reportar cualquier incidente sospechoso al CISRT Salud y a las autoridades competentes para facilitar la coordinación y respuesta sectorial.

La adopción de estas medidas es esencial para proteger la infraestructura tecnológica y la información sensible de las entidades de salud frente a la amenaza creciente del ransomware GUNRA.

Fuentes:

- https://www.bugsfighter.com/es/remove-gunra-ransomware-and-decrypt-encrt-files/