CORMAGDALENA
La energía de un río que impulsa a un país

Número Rad:	2022-300-2789	Fecha:	9/9/2022 9:33:12 AM
Trámite:	Comunicación de salida	Destino:	Dirección Seccional de Fiscalías
Origen:	Secretaria General	Folios:	1/4

Señor(a):
Dirección Seccional de Fiscalías del Magdalena Medio
BARRANCABERMEJA CR 56 18 A 80 P 10

Asunto: FORMULACIÓN DE DENUNCIA PENAL EN CONTRA DE INDETERMINADOS, VÍCTIMA: CORMAGDALENA.

Cordial saludo,

MARCELA GUEVARA OSPINA, identificada con la cédula de ciudadanía número 52.257.121 de Bogotá D.C, nombrada mediante Resolución 000313 del 22 de octubre de 2018 y posesionada a partir del 01 de noviembre de la misma anualidad mediante Acta No.241 en el cargo de Secretaria General de la Corporación Autónoma Regional del Río Grande de la Magdalena – CORMAGDALENA, entidad de la Administración Pública del orden Nacional, creada por el artículo 331 de la Constitución Política y reglamentada mediante la Ley 161 de 1994, identificada con NIT No. 829.000.127-4, cuya sede principal esta ubicada en la ciudad de Barrancabermeja (Santander) en la Carrera 1ra No. 52 - 10 Sector Muelle, me permito dirigirme a su despacho para denunciar las presuntas conductas punibles de: ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO, OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN, DAÑO INFORMATICO AGRAVADOS y los que se evidencien en el transcurso de la investigación, con base en los siguientes:

HECHOS:

1.Mediante comunicación interna No. 2022-100-2088 del 06 de septiembre de 2022 (anexo 1), los apoyos de sistemas de la entidad, ponen en conocimiento formal de la Secretaría General de la Entidad, los hechos ocurridos en los servidores de la entidad el día 30 de agosto de 2022, los cuales pasan a relacionarse

2.Se indica en el informe adjunto que siendo las 7:30 del día 30 de agosto de 2022 se realizó verificación del sitio web "www.cormagalena.gov.co"de la entidad y se encontraba caído (Fuera de servicio) y que, al ingresar por acceso remoto a la estación de trabajo donde se administran todos los servidores de la corporación para poder a través de este conectarse al servidor donde esta alojada la página web se encontró el pantallazo del informe adjunto a la presente denuncia.

3.Así mismo, el informe en referencia señala que al empezar a explorar el servidor ninguno de los archivos contenidos en carpetas del sitio web se encontraban normales, los nombres de los documentos y archivos.php habían sido modificados con la siguiente extensión: [Writeme100@tuta.io].LIZARD, de esta manera quedaron todos los nombres de archivos contenidos en el servidor, identificando que era un virus el cual afectó las siguientes extensiones de archivos:

- texto: txt, doc, docx, etc.
- imagen: jpg, gif, bmp, png, etc.
- vídeo: avi, mp4, mpeg, mwv, etc.
- audio: mp3, wav, wma, etc.
- archivo comprimido: zip, rar, etc.

CALIA

VENTANILLA UNICA DE CORRESPONDENCIA BARRACABERMEJA
DSMM-MC-GIT - No. 20227420041932
Fecha Radicado: 2022-09-09 15:16:39
Anexos: 2 FOLIOS + 5 ANEXOS

4.De igual forma , refiere el informe que el ransomware eliminó el gestor de la base de datos de la página web sin permitir consultar la fuente de los archivos sql y .php del portal de Cormagdalena, haciendo imposible su recuperación.

5.En este mismo sentido, el virus afectó el servidor del directorio activo con las mismas características del servidor web y modificó los nombres de todos archivos por la extensión: **Writeme100@tuta.io].LIZARD** . En este servidor reposaba la información de cartera que es

Oficina Principal
Barrancabermeja
Carrera 1 No. 52 - 10
Sector Muelle
PBX: (7) 6214422
FAX: (7) 6214507

Oficina Gestión y Enlace - Bogotá
Calle 93B No. 17 - 25
Oficina 504
PBX: (1) 6369093
FAX: (1) 6369052

Oficina Seccional
Barranquilla
Vía 40 No. 73 - 290
Oficina 802
PBX: (5) 3565914

MINISTERIO DE TRANSPORTE