EN LO PRINCIPAL: Diligencia que indica sin conocimiento de los afectados y antes de la formalización de la investigación;
PRIMER OTROSÍ: Copia simple
SEGUNDO OTROSÍ: Reserva y custodia;
TERCER OTROSÍ: Forma de notificación;

[redacted]

CRISTIAN ANDRES SUAREZ PEREZ,abogado, Fiscal Adjunto de la Fiscalía de Alta Complejidad y Crimen Organizado de la Fiscalía Regional Metropolitana Sur del Ministerio Público, en causa RUC [redacted] por el delito de SABOTAJE INFORMATICO, a S.S. respetuosamente digo:

Se ha tomado conocimiento de que una persona de nacionalidad chilena usuaria de los correos [redacted] habría elaborado un malware identificado con el [redacted] con el que se habrían realizado ataques informáticos tanto en Chile como en el extranjero, según antecedentes aportados por el FBI.

El virus individualizado con anterioridad, fue reconocido como malware por 43 proveedores de ciberseguridad, destacando que este tendría funciones que le permitirían capturar y encriptar archivos de sus víctimas, para efectos de cobrar un rescate a través de criptomomedas, condición que eventualmente permitiría la liberación de los archivos encriptados.

En éste sentido, la Fiscalía recibió [redacted] denuncia cursada por [redacted] quien se desempeña [redacted] quien señala:

"En primera instancia debo manifestar que [redacted] *ubicada* [redacted]

"En relación a los hechos que vengo a denunciar, debo señalar que el [redacted] *los sistemas de la empresa para revisar* [redacted] *no pudiendo ingresar,* [redacted] *contactarme al servidor para ver que ocurría, lugar en donde me aparece un mensaje en inglés, del cual me solicitan un*

rescate en Bitcoin para poder restaurar los sistemas, los cuales estaban encriptados. [redacted] *Desconozco antecedentes sobre cómo pudo ingresar el virus al sistema,* [redacted]

De acuerdo a lo señalado también se ha podido establecer que el virus con funciones criptográficas y eventualmente de minado de criptomonedas, se conecta con tres dominios:

[redacted]

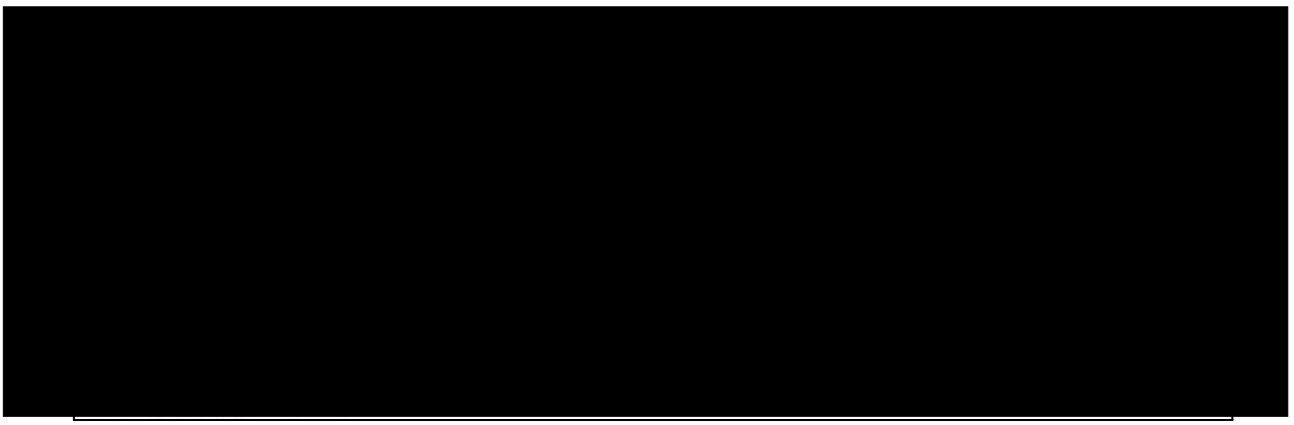
I. DETECCIÓN DEL VIRUS.

Con fecha [redacted] se consultó el [redacted] plataforma [redacted] logrando establecer que 43 de 69 proveedores de seguridad informática, identifican el código asociado al hash como malicioso.

[redacted]

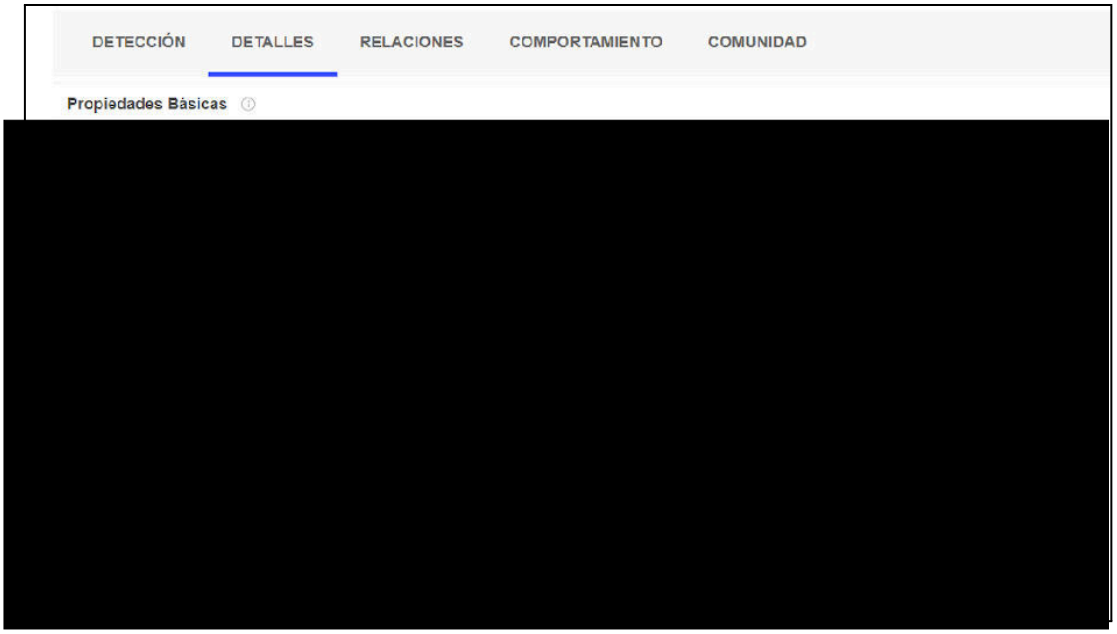
Se hace presente que haciendo uso de la plataforma “Virustotal”, se realizó un análisis del malware singularizado con el [redacted], destacando que la misma posee un ítem que alude a reglas SIGMA de colaboración colectiva (SIGMA, es un sistema estructurado para describir métodos de detección de

amenazas en Ciberseguridad). En el registro señalado se advierte coincidencias para lo que sería un *ranzomware*denominado “Nibiru”.



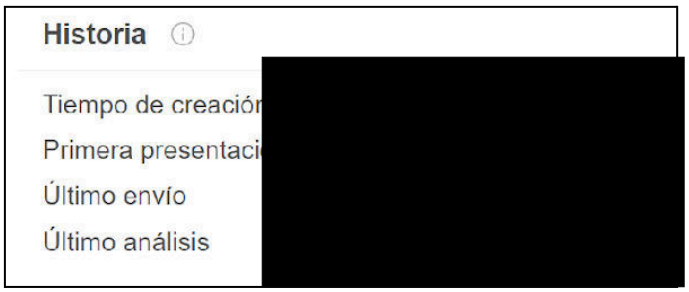
De igual forma, se advierte que de acuerdo a las reglas IDS (sistema de detección de intrusiones, utilizada para detectar accesos no autorizados a un ordenador o a una red) existen antecedentes que vinculan a este virus con la minería de criptomonedas.

Continuando con las indagatorias, y haciendo revisión de la información obtenida por intermedio se revisaron las propiedades básicas del malware, destacando lo siguiente:

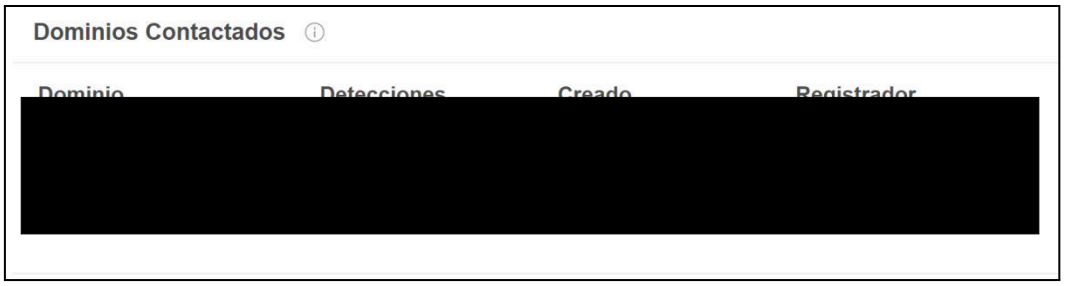


Entre los antecedentes a destacar que se obtienen a raíz de las propiedades señaladas en el recuadro, es la función criptográfica [redacted] ue es un sistema de encriptado de información, incluso [redacted] e utiliza en el proceso de minería de bitcoin, por el nivel de seguridad que ofrece.

De acuerdo a la historia de este malware, se advierte que su fecha o tiempo de creación sería e[redacted]



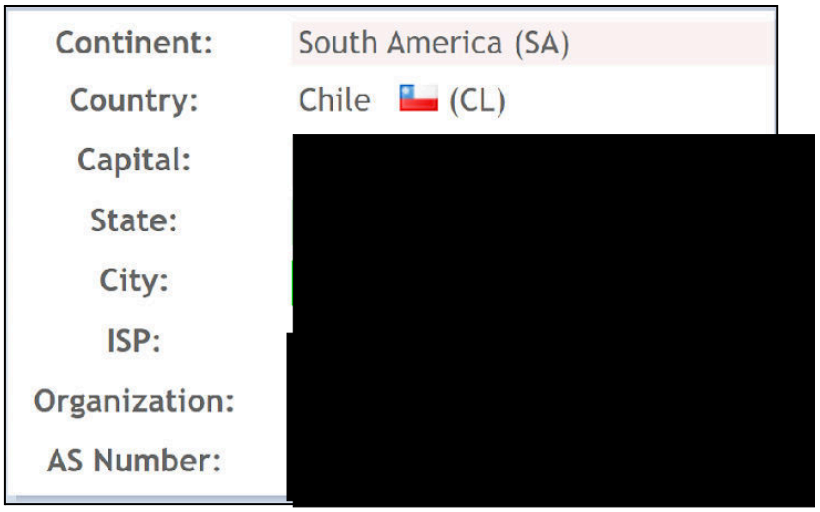
Respecto a las relaciones, se puede apreciar que este malware tiene conexión con [redacted] dominios [redacted]



Se hace presente, que consultados los dominios en “who.is”, estos fueron registrados por el proveedor de dominios En relación al contacto de registro, técnico o administrativo cuentan con protección de privacidad.

Continuando con las indagatorias ara efectos de siguientes resultados:

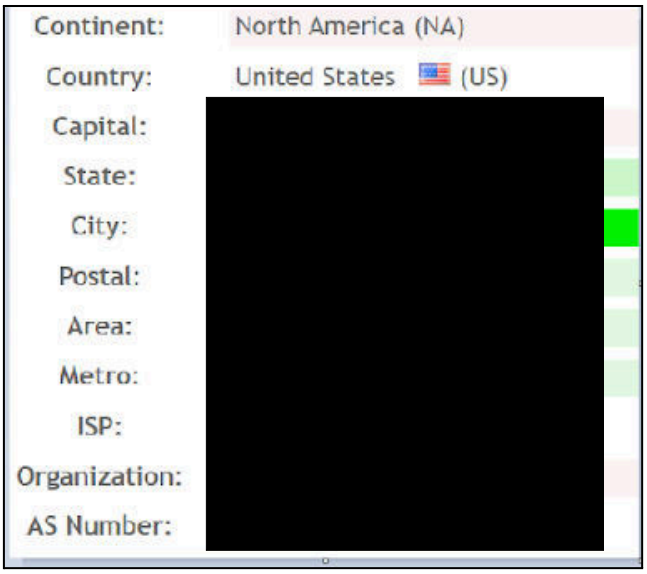
En relación a la dirección IP fue consultada en la plataforma IP Tracker logrando establecer que fue otorgada para el territorio nacional por el proveedor de servicios de internet



[redacted]

[redacted]

En relación a la dirección IP [redacted] esta fue consultada en la plataforma IP Trac[redacted] ogrando establecer que fue otorgada para el territorio de Estados Unidos por el proveedor de servicios de [redacted]



[redacted]

[redacted]

En relación a la dirección IP [redacted] esta fue consultada en la plataforma IP Tracker [redacted] logrando establecer que fue otorgada para el territorio de Estados Unidos por el proveedor de servicios de [redacted]

Continent:	North America (NA)
Country:	United States (US)
Capital:	[redacted]
State:	
City:	
Postal:	
Area:	
Metro:	
ISP:	
Organization:	

Continuando con las indagatorias, el día [redacted] se buscó información del virus Nibirus encontrando la siguiente información:

[redacted]

Resumen de amenazas: [redacted]	
Nombre	virus nibiru
Tipo de amenaza	Ransomware, virus criptográfico, casillero de archivos.
Extensión de archivos cifrados	.Nibiru
Mensaje de demanda de rescate	Pantalla bloqueada.
Cantidad de rescate	$4.5 millones en Bitcoins.
Contacto cibercriminal	cyberwars@protonmail.com
Nombres de detección	AVG (FileRepMalware), BitDefender (Generic.Ransom.CloudSword.05CC35B1), ESET-NOD32 (Una variante de MSIL/Filecoder.FG), Kaspersky (UDS:DangerousObject.Multi.Generic). Lista completa de detecciones (VirusTotal).
Síntomas	No puede abrir archivos almacenados en su computadora, los archivos anteriormente funcionales ahora tienen una extensión diferente (por ejemplo, my.docx.locked). Se muestra un mensaje de demanda de rescate en su escritorio. Los ciberdelincuentes exigen el pago de un rescate (generalmente en bitcoins) para desbloquear sus archivos.
información adicional	Este ransomware bloquea la pantalla de la víctima.
Métodos de distribución	Archivos adjuntos de correo electrónico infectados (macros), sitios web de torrents, anuncios maliciosos.
Daño	Todos los archivos están encriptados y no se pueden abrir sin pagar un rescate. Se pueden instalar troyanos que roban contraseñas adicionales e infecciones de malware junto con una infección de ransomware.

II. BLANCO INVESTIGATIVO.

Respecto a los correos [redacted] y [redacted] al imputadose buscó información de acuerdo al siguiente detalle:

En alusión [redacted] se indagó en el registro civil respecto al presunto nombre que se desprende de la casilla email, encontrando coincidencias con una persona individualizad[redacted]

[redacted]

que uno de sus parámetros es el corre[redacted]

También se logró encontrar información relacionada al siguiente sitio vinculado a la cuenta de correo:

[redacted]

Es del caso, que para efectos de que el virus ataque y/o infecte otros ordenadores requiere [redacted] encriptar archivos de sus víctimas o funciones que permitan generar un rescate en Bitcoin [redacted]

En virtud de lo anterior, [redacted] se hace imprescindible obtener autorización de US., con el objeto [redacted]

POR TANTO, de conformidad con lo dispuesto en el artículo 9, 205, 217, y 218 del Código Procesal Penaly los antecedentes expuestos;

PIDO A S.S., Se sirva autorizar [redacted]

PRIMER OTROSÍ: se sirva otorgar al suscrito copia simple de la resolución de este escrito como igualmente de los oficios solicitados

[redacted]

CRISTIAN SUAREZ PEREZ

Fiscal Adjunto de la Fiscalía de Alta Complejidad y Crimen Organizado

Fiscalía Regional Metropolitana Sur