Ministerio del Interior y Seguridad Pública
Gobierno de Chile
Subsecretaría del Interior
Unidad de Participación Ciudadana y Oficina de Transparencia

LEY 20.285 TRANSPARENCIA

ORD Nº : 13.327
MAT : Solicitudes N°s AB001T0000817 – AB001T0000822
ANT : Solicitud de Información Ley 20.285

SANTIAGO, 02 DE MAYO DE 2019

DE : SUBSECRETARIO DEL INTERIOR

A : [redacted]

Con fecha 08 y 10 de abril de 2019, se han recibido las siguientes solicitudes de acceso a la información N°s AB001T0000817 - AB001T000822 en las que se expone lo siguiente: *"Estimados,*

De acuerdo a lo notificado por el CSIRT del Ministerio de Interior y Seguridad Pública los días 22 y 23 de marzo del presente año en materia de potencial riesgo de infección por malware. Hemos encontrado como parte de la sociedad civil que es competente generar una investigación sobre la rigurosidad que el proceso debe tener para la generación de estos tipos de notificaciones.

En este contexto hemos decidido comenzar una investigación en relación a las amenazas que están activas en el contexto chileno y sus repercusiones, tanto a nivel gubernamental como privado.

Para ello, nos gustaría que nos faciliten información relativa a lo siguiente:
- Información del origen de esta notificación.
- Procedimiento de análisis sobre la información notificada.
- Información obtenida por dicho procedimiento.
a) Proceso en donde se identifican los IOC relacionados con EMOTET.
b) Proceso ocupado para identificar que los IOC interactúan con la vulnerabilidad de Winrar.
c) Proceso en el cual se define la severidad de las amenazas.
- Procedimiento y autoridades que se relacionan, en la actualidad, en la aprobación de la notificación de un incidente de estas características.
- ¿En la actualidad se posee con un procedimiento de administración de crisis?

1741465

Esta información es de vital ayuda a nuestra investigación, ya que verificará el estado de madurez que en la actualidad se posee para la generación de estos tipos de notificación.

Sin otro particular, esperando una buena acogida.

Se despide,

[redacted] *- Presidente de Fundación de Investigación en Seguridad Informática (FINSIN)*

[redacted] *- Presidente de Fundación Educacional WHILOLAB*

[redacted] *- Presidente de la comunidad de Seguridad Informática PartyHack*

[redacted] *- Responsable de exploiting.cl".*

Al respecto, cabe advertir que, de acuerdo a lo dispuesto en el inciso segundo, del artículo 10, de la ley Nº 20.285, sobre Acceso a la Información Pública, éste último comprende el derecho a acceder a la información contenida en actos, resoluciones, actas, expedientes, contratos y acuerdos, así como a toda información elaborada con presupuesto público, cualquiera sea su formato o soporte. En este sentido, debe destacarse que la ley Nº 20.285, permite acceder a información que, al momento de la solicitud, obre en poder del órgano de la Administración Pública requerido, y esté contenida en algún soporte, sin importar cuál sea éste; siendo dable agregar que, en todo caso, el citado texto legal no obliga a los organismos públicos a generar, elaborar o producir información, sino a entregar la actualmente disponible.

Aclarado lo anterior, y en lo que concierne al requerimiento formulado en la especie, esta Subsecretaría del Interior le comunica lo siguiente:

1. Es del caso contextualizar, que su petición se centra en el proceso para la generación del comunicado realizado por el Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT) dependiente de este Ministerio con fecha 22 y 23 de marzo del 2019 sobre un potencial riesgo de infección realizado por un malware (EMONET), y en ese contexto, cabe indicar que el equipo indicado, publicó dos comunicados en que se expresaba el nivel de alerta asociado a las amenazas que estaban afectando a diferentes entidades, indicando lo que se debería hacer dado el nivel de propagación y afectación en que estaban incurriendo ciertas instituciones, sectores de la industria y el riesgo que esto podría provocar en el resto de los sistemas informáticos nacionales.
2. En ese orden de ideas, le informamos que la información que usted requiere, proviene de múltiples fuentes con las que el Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT) tiene convenios, acuerdos, servicios

contratados, instancias de colaboración con otros órganos, así como también, con otras instituciones nacionales e internacionales, y en ese contexto, cada convenio con las entidades colaboradoras contempla cláusulas de confidencialidad.

3. Luego, dado que a juicio de esta Subsecretaría, los procedimientos de análisis son sensibles para la seguridad y estabilidad de la Red Gubernamental, y dado que es posible que con el conocimiento de esta información se revelaran antecedentes trascendentes para el normal desarrollo estratégico en materia de ciberseguridad del Ministerio del Interior y Seguridad Pública, afectando con ello, todas aquellas unidades conectadas a la Red de Conectividad del Estado.
4. Ahora bien, y con respecto a la última parte de su requerimiento en el cual solicita información sobre el *"- Procedimiento y autoridades que se relacionan, en la actualidad, en la aprobación de la notificación de un incidente de estas características. - ¿En la actualidad se posee con un procedimiento de administración de crisis?"*, le indicamos que el procedimiento es actualmente operado por equipos del Ministerio del Interior y Seguridad Publica, y del Ministerio de Defensa Nacional, quienes son también, los actores que validan las notificaciones de incidentes, existiendo al efecto, un procedimiento de administración de crisis, con carácter de reservado, activándose, y escalando según el incidente reportado. Por ello, es que, necesariamente los procedimientos de análisis son sensibles para la Seguridad y estabilidad de la Red Gubernamental y por ende, de la Nación misma, dado que la publicidad de esta información, necesariamente revelaría antecedentes trascendentales para el normal desarrollo estratégico en materia de ciberseguridad del Ministerio del Interior y Seguridad Pública, afectando, como necesaria consecuencia la seguridad de las redes del Estado.
5. Es por lo antes indicado, que es del caso puntualizar que, el artículo 21, N° 3, letra c), de la ley N° 20.285, dispone que constituye causal para denegar una solicitud de acceso a la información, *"cuando su publicidad, comunicación o conocimiento afecte a la seguridad de la Nación, particularmente si se refiere a la defensa nacional o la mantención del orden público o a la seguridad pública"*. En este sentido, y de acuerdo a lo informado por la División Informática de esta Subsecretaría, la entrega de información requerida, implicaría necesariamente una gravísima vulneración, por cuanto, dicha información, como ya se indicó, se considera sensible para la seguridad y estabilidad de la Red Gubernamental, y por ende, es necesario darle tratamiento de bien jurídico colectivo susceptible de protección.

   Por lo tanto, si bien esta Subsecretaría de Estado, mediante la aplicación del principio de transparencia de la función pública, prevista en el artículo 11, letra c), de la ley N° 20.285, se encuentra siempre llana a acoger las solicitudes de transparencia efectuadas por la ciudadanía, lamentablemente, en esta parte de su solicitud, no es posible acceder por las razones expuestas en los párrafos precedentes.

Luego, y en cumplimiento de la Instrucción General N° 10, cumplo con informarle que usted puede interponer amparo a su derecho de acceso a la información ante el Consejo para la Transparencia, dentro de un plazo de 15 días hábiles contado desde la notificación del presente oficio.

INCORPÓRESE el presente oficio al Índice del artículo 23, de la Ley N° 20.285, una vez que se encuentre firme.

Finalmente y por razones de buen servicio, le sugerimos visitar los siguientes sitios webs, en los cuales, de conformidad al artículo 15° de la Ley de Transparencia, se encuentra publicada información que podría ser su interés, dado que guarda relación con el objeto de su petición.

a. [https://www.csirt.gob.cl/]
b. [https://www.ciberseguridad.gob.cl/]

Saluda atentamente a Ud.

REPUBLICA DE CHILE SUBSECRETARIO MINISTERIO DEL INTERIOR Y SEGURIDAD PUBLICA

RODRIGO UBILLA MACKENNEY
SUBSECRETARIO DEL INTERIOR

PMV/JCI
DISTRIBUCIÓN:
1) [redacted]
2) Gabinete Subsecretario del Interior
3) Oficina de Partes

Detalle de Solicitud: AB001T0000817

Estado Solicitud	Solicitud en Trámite	**Fecha Ingreso**	08/04/2019

Detalle Formulario

Tipo Solicitud	Acceso a Información (Ley20285)	**Vía de Ingreso**	Web
Materia			
Temática			
Programa			
Estado	Solicitud en Trámite		

Detalle Solicitud

Estimados, De acuerdo a lo notificado por el CSIRT del Ministerio de Interior y Seguridad Pública los días 22 y 23 de marzo del presente año en materia de potencial riesgo de infección por malware. Hemos encontrado como parte de la sociedad civil que es competente generar una investigación sobre la rigurosidad que el proceso debe tener para la generación de estos tipos de notificaciones. En este contexto hemos decidido comenzar una investigación en relación a las amenazas que están activas en el contexto chileno y sus repercusiones, tanto a nivel gubernamental como privado. Para ello, nos gustaría que nos faciliten información relativa a lo siguiente: - Información del origen de esta notificación. - Procedimiento de análisis sobre la información notificada. - Información obtenida por dicho procedimiento. a) Proceso en donde se identifican los IOC relacionados con EMOTET. b) Proceso ocupado para identificar que los IOC interactúan con la vulnerabilidad de Winrar. c) Proceso en el cual se define la severidad de las amenazas. - Procedimiento y autoridades que se relacionan, en la actualidad, en la aprobación de la notificación de un incidente de estas características. - ¿En la actualidad se posee con un procedimiento de administración de crisis? Esta información es de vital ayuda a nuestra investigación, ya que verificará el estado de madurez que en la actualidad se posee para la generación de estos tipos de notificación. Sin otro particular, esperando una buena acogida. Se despide, [redacted]- Presidente de Fundación de Investigación en Seguridad Informática (FINSIN)[redacted]- Presidente de Fundación Educacional WHILOLAB [redacted]- Presidente de la comunidad de Seguridad Informática PartyHack[redacted]- Responsable de exploiting.cl

Observaciones	
Usuario desea respuesta mediante:	ELEC

Datos Solicitante

Detalle de Solicitud: AB001T0000822

Estado Solicitud	En proceso de recopilación de Información	**Fecha Ingreso**	10/04/2019

Detalle Formulario

Tipo Solicitud	Acceso a Información (Ley20285)	**Vía de Ingreso**	Web
Materia			
Temática			
Programa			
Estado	En proceso de recopilación de Información		
Detalle Solicitud	Estimados, De acuerdo a lo notificado por el CSIRT del Ministerio de Interior y Seguridad Pública los días 22 y 23 de marzo del presente año en materia de potencial riesgo de infección por malware. Hemos encontrado como parte de la sociedad civil que es competente generar una investigación sobre la rigurosidad que el proceso debe tener para la generación de estos tipos de notificaciones. En este contexto hemos decidido comenzar una investigación en relación a las amenazas que están activas en el contexto chileno y sus repercusiones, tanto a nivel gubernamental como privado. Para ello, nos gustaría que nos faciliten información relativa a lo siguiente: - Información del origen de esta notificación. - Procedimiento de análisis sobre la información notificada. - Información obtenida por dicho procedimiento. a) Proceso en donde se identifican los IOC relacionados con EMOTET. b) Proceso ocupado para identificar que los IOC interactúan con la vulnerabilidad de Winrar. c) Proceso en el cual se define la severidad de las amenazas. - Procedimiento y autoridades que se relacionan, en la actualidad, en la aprobación de la notificación de un incidente de estas características. - ¿En la actualidad se posee con un procedimiento de administración de crisis? Esta información es de vital ayuda a nuestra investigación, ya que verificará el estado de madurez que en la actualidad se posee para la generación de estos tipos de notificación. Sin otro particular, esperando una buena acogida. Se despide, [redacted]- Presidente de Fundación de Investigación en Seguridad Informática (FINSIN) [redacted]- Presidente de la comunidad de Seguridad Informática PartyHack [redacted]- Responsable de exploiting.cl		
Observaciones			
Usuario desea respuesta mediante:	ELEC		

Datos Solicitante