LOCKY: NUEVO RANSOMWARE CON CARACTERÍSTICAS COMUNES AL TROYANO BANCARIO DRIDEX

| 19 Feb, 2016 | Ransomware | No hay comentarios

El uso del ransomware como vía para obtener dinero fácil por parte de los delincuentes se ha estado incrementando durante los últimos meses. Prueba de ello son las numerosas variantes que han ido apareciendo durante las últimas semanas, variantes que en ocasiones van acompañadas de una importante campaña de propagación para intentar obtener el mayor número de víctimas posible.

PROPAGACIÓN POR EMAIL DE UN DOCUMENTO MALICIOSO

Una de estas campañas se está produciendo durante esta semana, concretamente desde el martes 16 de febrero, a través de mensajes de correo electrónico en inglés que nos hablan de una supuesta factura. Esta factura viene adjunta al mensaje en forma de un documento de Microsoft Word, tiene como nombre InvoiceXXXXXX.doc (donde XXXXXX es un número aleatorio).

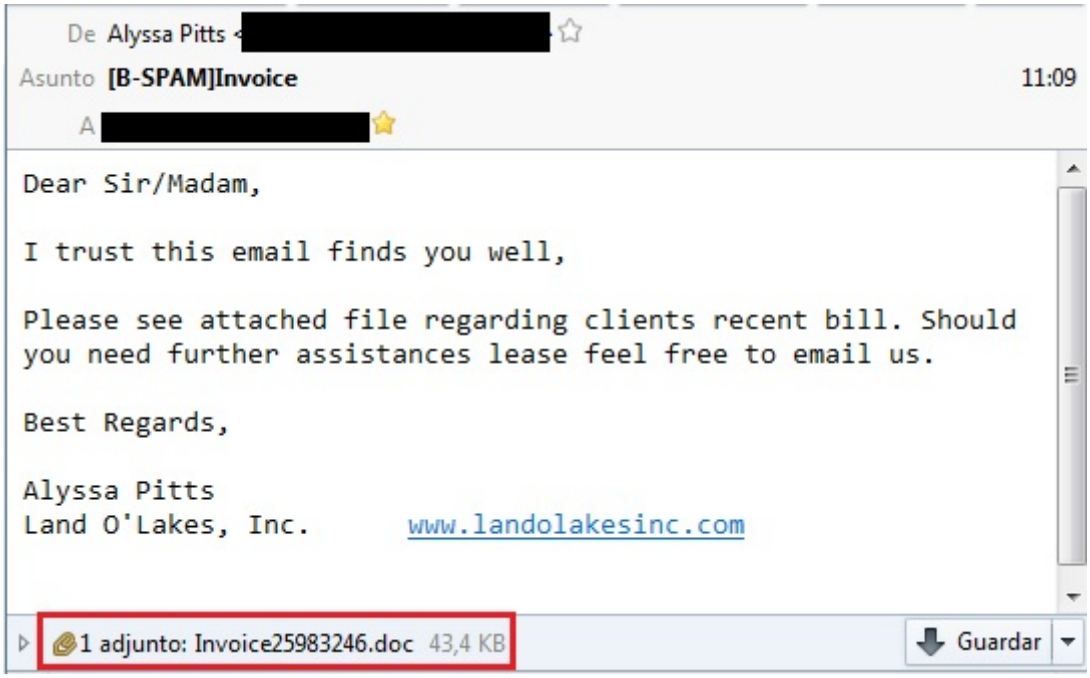

Imagen1 – Ejemplo de correo con adjunto malicioso

Los remitentes pueden ser usuarios de cualquier parte del mundo, por lo que estamos ante una campaña global, aunque, como veremos más adelante, su éxito depende del país o región que analicemos.

Si descargamos el fichero adjunto y lo descomprimimos, observaremos que aparentemente se trata de un inofensivo documento de Microsoft Word, el conocido procesador de textos de la suite de Office.

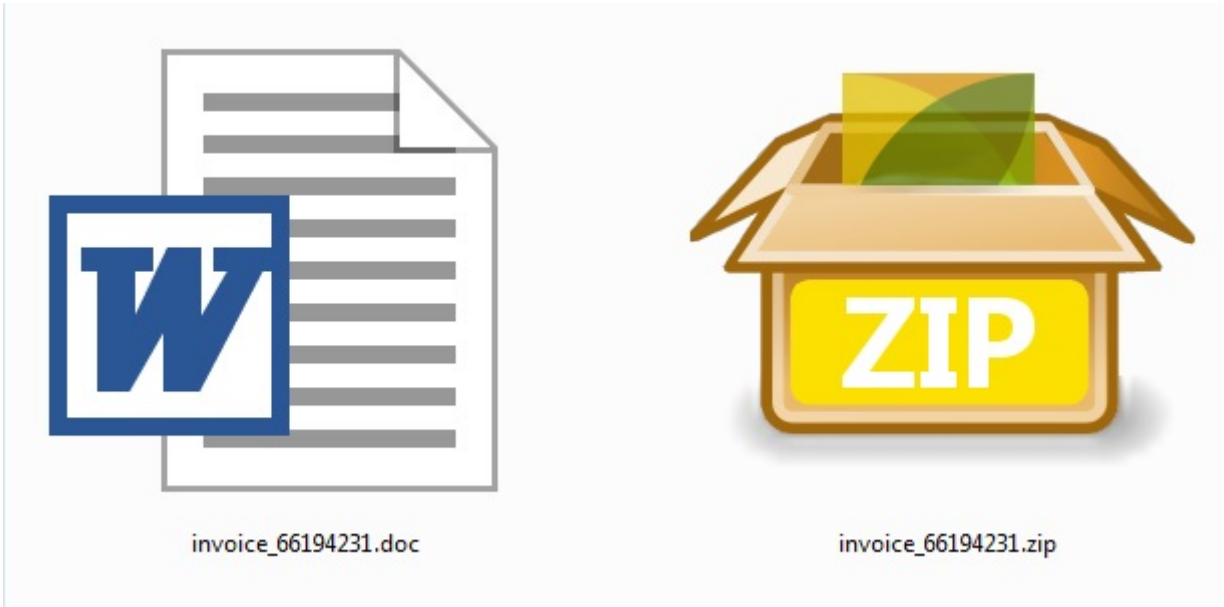

Imagen 2 – Ejemplo de documento Word malicioso

La trampa se encuentra dentro de ese documento, puesto que los delincuentes utilizan macros maliciosas para descargar y ejecutar el ransomware. Estas macros vienen desactivadas por defecto como medida de seguridad, y es que esta técnica de ejecución de malware es algo que viene existiendo desde hace casi 20 años.

LOCKY EN ACCIÓN

Si hemos sido lo suficientemente desprevenidos para descargar este documento, abrirlo y permitir la ejecución de macros, nos encontraremos con que, al cabo de unos minutos, gran parte de los ficheros de nuestro sistema estarán cifrados y aparecerá una imagen como la que vemos a continuación sustituyendo nuestro fondo de pantalla:

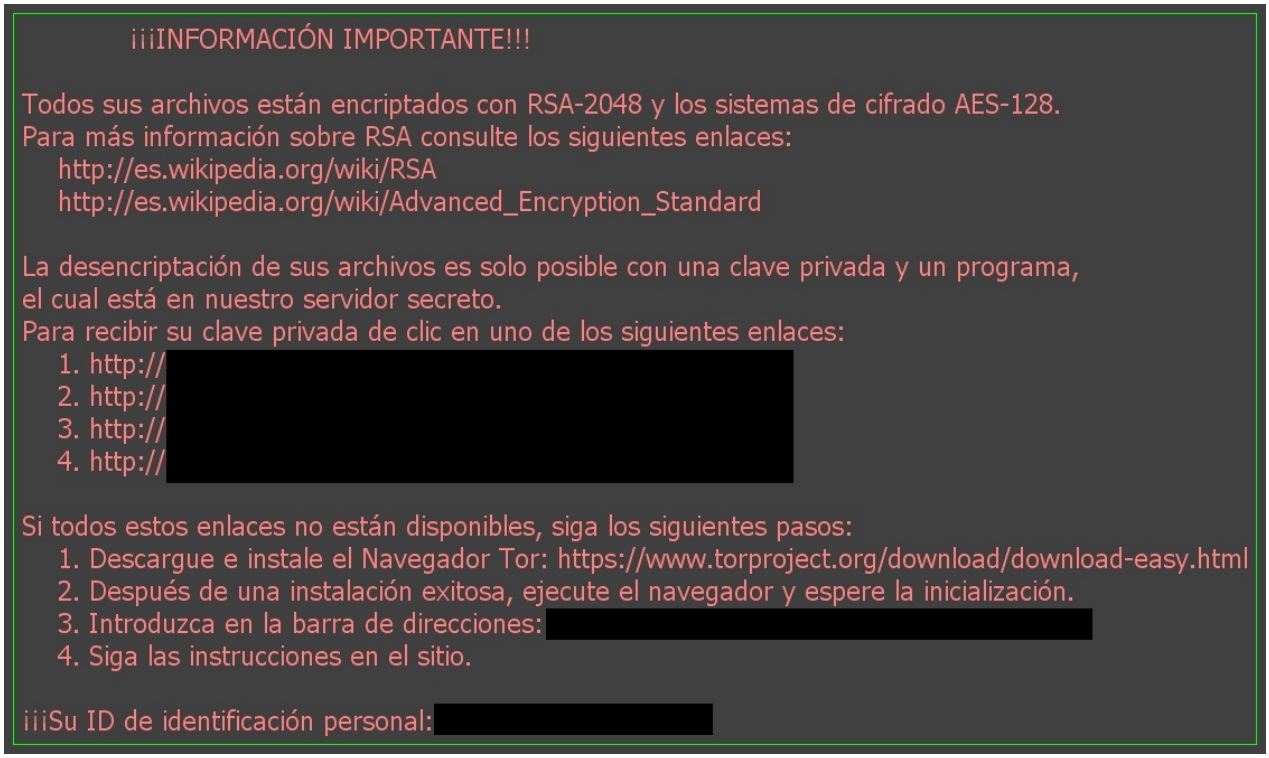

Imagen 3 – Fondo de pantalla avisando del secuestro de nuestros ficheros

Si nos fijamos, este tipo de instrucciones es muy similar a variantes anteriores de ransomware. En esta pantalla se nos proporcionan varios enlaces donde se explica el tipo de cifrado usado, una dirección desde donde poder recibir la clave privada correspondiente a los ficheros cifrados en nuestro sistema, e instrucciones para descargar Tor y acceder a un sitio en esta red desde donde proceder a pagar el rescate.

En este punto, los ficheros que no sean esenciales para el funcionamiento del sistema ya estarán cifrados. Los tipos de ficheros que busca Locky en nuestro sistema van desde las imágenes a los documentos y abarcan prácticamente cualquier archivo que pueda tener un mínimo valor para el

usuario. Sin embargo, se cuida mucho de no cifrar aquellos archivos que resulten esenciales para el funcionamiento del sistema, de forma que la víctima pueda seguir las instrucciones.

Además, Locky no se centra únicamente en cifrar los ficheros del sistema que infecta, sino que también buscará unidades de red, aunque estas no se encuentren mapaeadas, para proceder a cifrarlas. Esta técnica se está volviendo cada vez más común, por lo que los administradores de sistemas de pequeñas y grandes empresas harían bien en revisar a qué usuarios conceden permisos de acceso a los recursos compartidos de red y bloquear lo antes posible a aquellos que ejecuten comandos de cifrados desde su sistema.

Otra característica que dificulta la recuperación de los datos es la eliminación de las Shadow Copies en el sistema. Si bien esta técnica se viene realizando desde hace tiempo, no deja de ser un problema no poder contar con las copias de seguridad generadas de forma automática por Windows.

Por último, en cada una de las carpetas donde se haya cifrado al menos un fichero, el ransomware deja un fichero de texto con instrucciones para recuperar la información, instrucciones que dirigen a la víctima a la siguiente página web para que realice el pago del rescate.

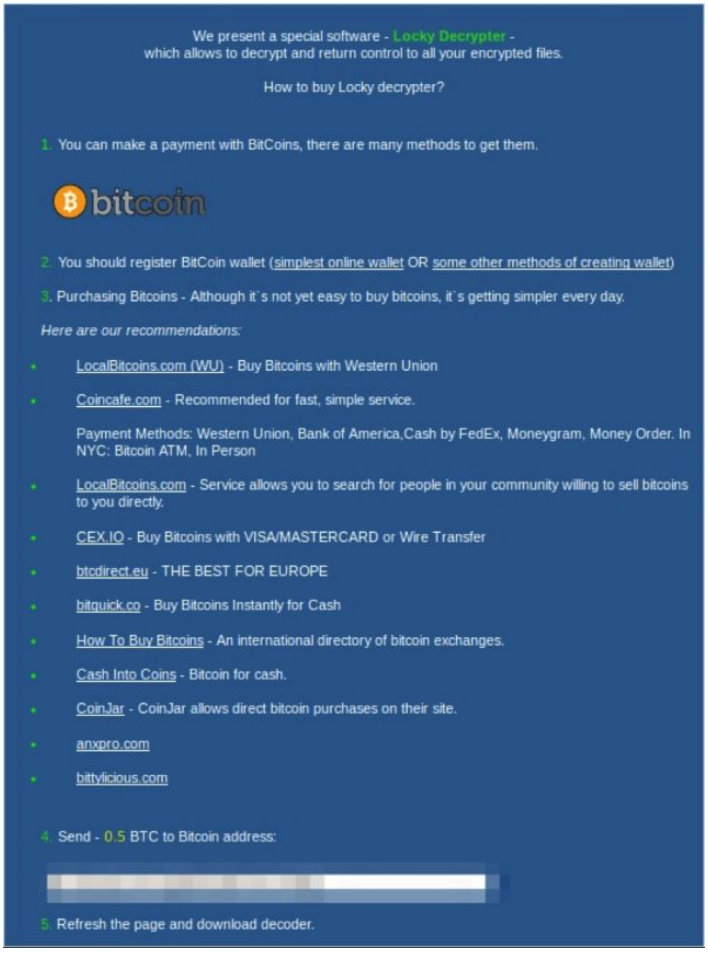

Imagen 4 – Instrucciones para proceder al pago del rescate

PROPAGACIÓN DE LOCKY A NIVEL MUNDIAL

Como hemos indicado anteriormente, nos encontramos ante una campaña de propagación que está afectando notablemente a varios países de todo el mundo. Los países en los que se han detectado el mayor número de muestras coinciden con algunas de las zonas más desarrolladas y encontramos, por ejemplo, a Canadá, Estados Unidos, Nueva Zelanda, Australia, Japón o buena parte de la Unión Europea.

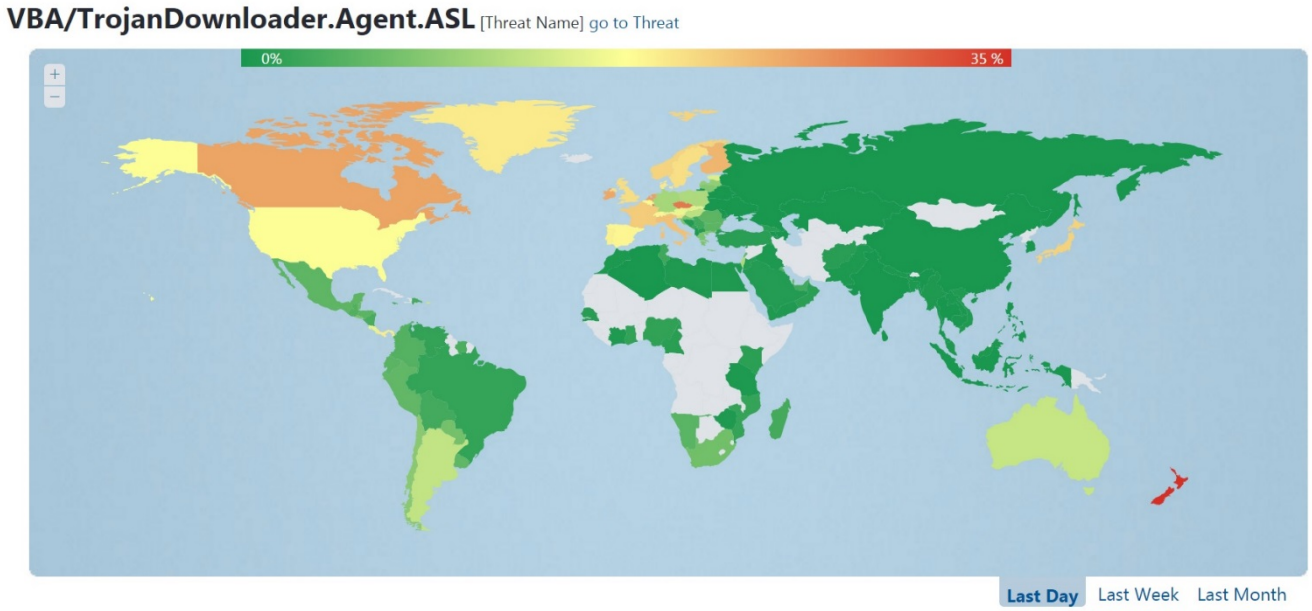

Imagen 5 – Niveles de propagación de Locky en el mundo

En lo que respecta a España, el documento de Word con las macros maliciosas que descarga el ransomware (detectado por las soluciones de ESET como VBA/TrojanDownloader.Agent.ASL) ha obtenido elevados ratios de detección tanto el miércoles 17 como el jueves 18 de febrero. Nuestra previsión es que permanezca unos días más en el puesto número 1 de las amenazas más detectadas, por lo que recomendamos tomar medidas de protección para evitar vernos afectados.

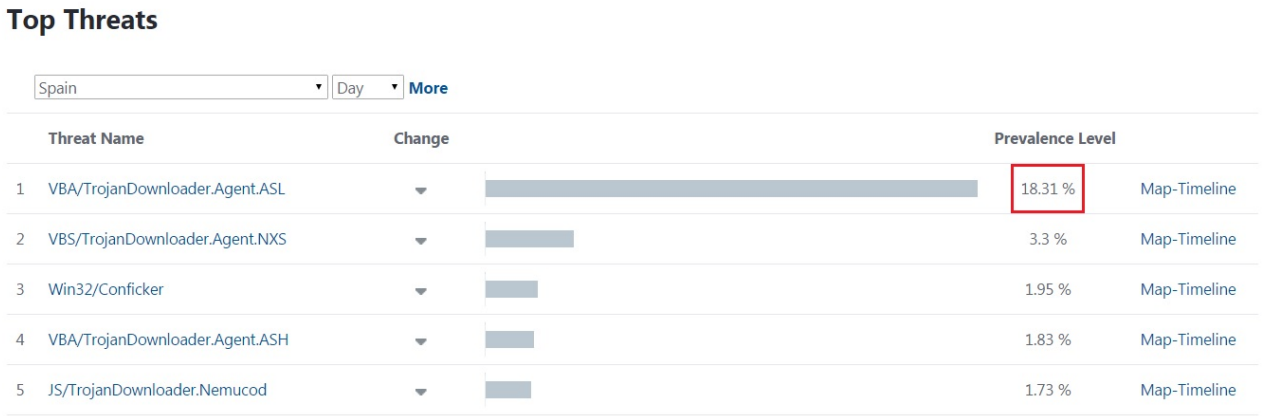

Imagen 6 – Porcentaje de detección de Locky en España

CONEXIONES CON OTRAS FAMILIAS DE MALWARE

Debido al diseño de este ransomware y su similitud con otras variantes avanzadas, se ha especulado mucho sobre quién podría estar detrás de esta campaña de propagación. Algunos expertos apuntan a que detrás de Locky podría estar la misma organización criminal que tanto daño ha causado con el troyano bancario Dridex.

Si bien es cierto que utiliza uno de los métodos de propagación que tan buenos resultados le ha dado a los creadores de Dridex, también hay que decir que hay muchas otras familias de malware que utilizan documentos de Microsoft Office con macros maliciosas para infectar a sus víctimas.

Además, algunos investigadores han descubierto que Locky también se está propagando usando los mismos identificadores que utiliza el kit de exploits Neutrino para propagar amenazas como Necurs. Por si fuera poco, en ambos casos los rescates apuntan a la misma cartera de Bitcoin y parece que utilizan la misma infraestructura.

Estas coincidencias pueden significar que ambas amenazas están siendo gestionadas y manejadas por el mismo grupo de delincuentes o que se está utilizando una distribución por medio de afiliados, algo bastante más probable viendo ejemplos recientes.

RECOMENDACIONES

Tal y como venimos comentando cada vez que analizamos un caso de ransomware, especialmente si su propagación es bastante elevada (como es el caso), resulta vital tomar las medidas de prevención adecuadas. Las copias de seguridad han de estar al día y desconectadas de la red una vez finalizadas para evitar que este ransomware también las cifre. De esta forma se podrá restaurar la información afectada sin mayores pérdidas que el tiempo que tardemos en realizar esta operación.

Además, contar con un antivirus que sea capaz de detectar nuevas variantes de malware de forma rápida, como las soluciones de ESET y su sistema LiveGrid, permite detectar este tipo de amenazas al poco tiempo de empezar a propagarse. Si esta protección la complementamos con herramientas específicas como AntiRansom instaladas en los sistemas que puedan verse afectados, conseguiremos que salten las alertas al primer indicio de actividad del ransomware.