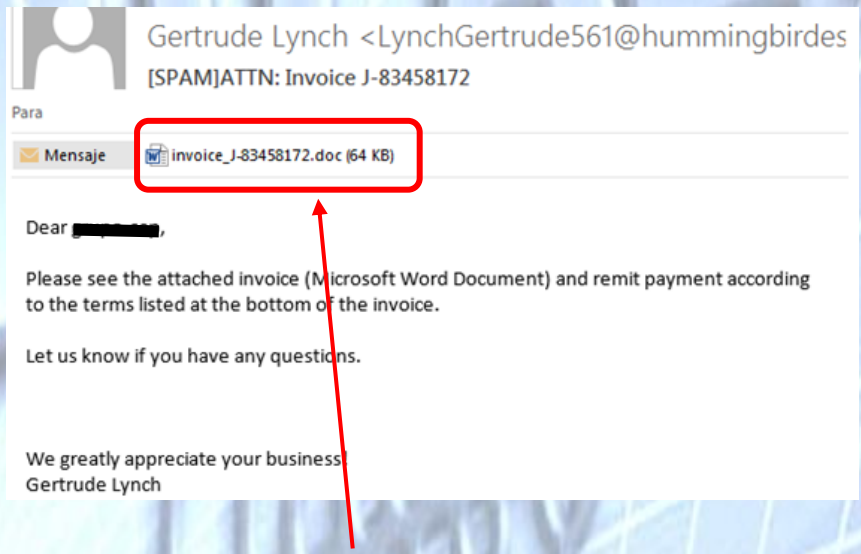
INFORMANDO DE INCIDENCIA DE NUEVA CAMPAÑA DE DISTRIBUCIÓN DE RANSOMWARE

Se acaba de detectar una campaña de correos maliciosos simulando provenir de una empresa extranjera con la que se tiene pendiente la realización de un pago, con aspectos similares al que se indica:



MUY IMPORTANTE NO ABRIR EL DOCUMENTO ADJUNTO QUE CONTIENE.

Estos e-mails parecen tener el común el asunto: ATTN:Invoice, y se insta a los destinatarios a descargarse un documento de Word que al ejecutar las macros que contiene, procede al cifrado de parte de los archivos del ordenador infectado con la extensión ".LOCKY", cambiando el nombre del archivo por un Id de usuario.

Las instrucciones que aporta el malware una vez ejecutado son las siguientes:

¡¡¡INFORMACIÓN IMPORTANTE!!!

Todos sus archivos están encriptados con RSA-2048 y los sistemas de cifrado AES-128.
Para más información sobre RSA consulte los siguientes enlaces:
http://es.wikipedia.org/wiki/RSA

http://es.wikipedia.org/wiki/Advanced_Encryption_Standard

La desencriptación de sus archivos es solo posible con una clave privada y un programa, el cual está en nuestro servidor secreto.

Para recibir su clave privada de clic en uno de los siguientes enlaces:
1. http://6dtxgqam4crv6rr6.tor2web.org/(ID_usuario afectado)
2. http://6dtxgqam4crv6rr6.onion.to/ (ID-usuario afectado)
3. http://6dtxgqam4crv6rr6.onion.cab/(ID-usuario afectado)
4. http://6dtxgqam4crv6rr6.onion.link/(ID-usuario afectado)

Si todos estos enlaces no están disponibles, siga los siguientes pasos:
1. Descargue e instale el Navegador Tor: https://www.torproject.org/download/download-easy.html
2. Después de una instalación exitosa, ejecute el navegador y espere la inicialización.
3. Introduzca en la barra de direcciones: 6dtxgqam4crv6rr6.onion/(ID-usuario afectado)
4. Siga las instrucciones en el sitio.

¡¡¡Su ID de identificación personal: (ID-usuario afectado)!!!

RECOMENDACIONES

Este tipo de malware suele transmitirse a través del correo electrónico, por lo que es muy importante seguir unas buenas prácticas como por ejemplo:

- **NUNCA** abrir links o descargar archivos de procedencia dudosa o desconocida.
- Realizar **copias de seguridad** frecuentes que posibiliten la recuperación de los archivos, **SIEMPRE guardarlas en un dispositivo independiente**, como puede ser un disco duro externo.
- Mantener el **Software y el antivirus siempre actualizado**.
- Mostrar extensiones de los archivos y **nunca ejecutar .EXE desconocidos**.
- **Utilizar el sentido común**, si se recibe un correo sospechoso, no abrirlo hasta contrastar su procedencia, incluso contactando con el supuesto remitente o la compañía de transporte.

Finalmente se desea transmitir que desde la experiencia de esta Unidad de Investigación Tecnológica, en determinados casos, el uso de un punto de restauración del sistema operativo anterior a la infección ha conseguido recuperar gran parte de los archivos encriptados.