Campaña masiva de correos con virus que suplantan identidad

El viernes 20/09/2019 se detectaron los primeros envíos de correo que contenían adjuntos Word con el virus identificado como Emotet. Su peligrosidad radica en que suplanta direcciones de usuarios reales, con el asunto y cuerpo del mensaje muy bien construidos.

España es uno de los países más afectados.

El Servicio de Informática recomienda extermar la precaución. La Oficina de Seguridad del Internauta también ha dado la alerta.

Están afectados todos los usuarios que reciban el correo electrónico, abran el archivo adjunto .doc infectado y **habiliten la edición o habilitar el contenido en Ms. Word**.

Imagen del archivo con virus

Detalles del mensaje

Existen diferentes variantes del mensaje con asuntos y contenido diferentes.

Como remitente del mensaje aparece una dirección de la Universidad de Jaén y a continuación otra externa.

from del mensaje

En el asunto del mensaje aparecen expresiones como:

- Nueva cesión de datos
- CONTRATO
- privacidad/PRIVACIDAD
- solicitud
- respuesta
- propuesta
- oferta solicitada
- Nueva plantilla

Y en el cuerpo tiene una apariencia similar a la siguiente captura:

Mensaje con virus

Como adjunto, aparece un archivo .doc con diferentes nombres y sin un patrón exacto.

- Adjunto 20190920 942323.doc
- Adjunto 20190722 343434.doc

La página de la Oficina de Seguridad del Internauta muestra más ejemplos de mensajes.

Solución

Los antivirus corporativos de la UJA ya **evitan** la infección de nuevos equipos. Sin embargo, no hay una solución definitiva para los equipos que **ya están infectados**. El Servicio de Informática sigue en contacto con los fabricantes a la espera de una herramienta adecuada.

Desde el martes 23 de septiembre, se están aplicando filtros en los sistemas de correo bloquean la salida y entrada de nuevos correos maliciosos relacionados con esta campaña.

La recomendación principal es no abrir archivos de word adjuntos incluidos en mensajes sospechosos y eliminarlos inmediatamente.

En cuanto el Servicio de Informática tenga información sobre la detección y eliminación del virus lo comunicará a la comunidad universitaria.