

Rgtº. Sº. Nº.: 230

---

### Aviso Instituto Nacional de Ciberseguridad

---

El Instituto Nacional de Ciberseguridad ha publicado un aviso sobre una campaña de correo electrónicos maliciosos destinados principalmente a empresas de arquitectura. A continuación reproducimos el contenido del aviso:

**[Campaña de correos electrónicos maliciosos que pretenden infectar equipos con ransomware](#)**

#### Fecha de publicación

28/08/2023

Importancia 4 - Alta

#### Recursos Afectados

Todo empresario, autónomo o empleado que haga uso del correo electrónico de empresa y reciba un mensaje con las características descritas en este aviso.

#### Descripción

Se ha detectado una nueva campaña de correos electrónicos fraudulentos que tratan de infectar los equipos de las empresas con un *ransomware*. La campaña detectada va dirigida a empresas de arquitectura, aunque no se descarta que su radio de acción se amplíe a otros sectores. Los ciberdelincuentes suplantan la identidad de una conocida empresa fotográfica solicitando un presupuesto con el que ganarse la confianza del destinatario y poder, finalmente, enviarle unos archivos infectados.

#### Solución

Si se recibe un correo electrónico como el que se describe en el aviso, se recomienda eliminarlo inmediatamente y ponerlo en conocimiento del resto de empleados, así como de las autoridades, para evitar posibles víctimas.

En caso de haber respondido al correo, haber recibido los archivos infectados y haberlos ejecutado, se recomienda desconectar el equipo de la red lo más pronto posible y cortar todo tipo de comunicación con el ciberdelincuente.

Nuestra recomendación es apagar el equipo cuanto antes con el objetivo de detener la propagación del cifrado de archivos que el malware está realizando. Tras ello, lo idóneo será contactar con un técnico que ofrezca asistencia para poder descifrar los archivos.



El [ransomware](#) es un malware que toma el control completo de los archivos que se encuentran en el equipo, cifrando dicha información a la espera de un rescate. Para aprender más sobre este tipo de ataque consulta el [siguiente blog](#) y no dejes que secuestren tu información.

#### Detalle

Varios trabajadores han recibido un correo fraudulento en el que se les solicita presupuesto para realizar una obra. Este correo, aparentemente legítimo, suplanta la identidad de una conocida empresa de fotografía y, en su nombre, solicita el presupuesto. Este primer correo aparenta ser real, ya que emplea una comunicación correcta y ajustada al destinatario. Esta técnica se conoce como ataque dirigido.

Madrid, 4 de septiembre de 2023

EL SECRETARIO GENERAL



Presidente/Presidenta del Colegio Oficial de Aparejadores y Arquitectos Técnicos.