DETECTADA CAMPAÑA DE *MALWARE EMOTET* EN CORREOS CORPORATIVOS

- **Organizaciones públicas y privadas están recibiendo emails con *malware EMOTET* en las cuentas de correo corporativas.**
- **Contiene un archivo adjunto en formato zip que no hay que abrir bajo ningún concepto.**

La Policía Nacional ha detectado una campaña de correos que adjuntan un archivo en formato zip, así como las contraseñas para abrirlo. En caso de ejecutarse, el dispositivo informático se infectará con ***EMOTET***, ***malware* tipo troyano.**

Nunca se debe abrir el archivo adjunto, recomendándose seguir las siguientes medidas preventivas:

RECOMENDACIONES:

- **Precaución a la hora de ejecutar cualquier tipo de adjunto o enlace.**
- **Tener especial cuidado con los correos de contactos conocidos,** ya que EMOTET puede suplantar su identidad.
- Si el correo contiene un **enlace a un sitio web, se analizará** utilizando las herramientas **VirusTotal y URLhaus.**
- **No habilitar una macro**, salvo que se esté **totalmente seguro de su legitimidad.**
- Tener los **sistemas actualizados** y utilizar **contraseñas robustas.**

Para obtener más información en relación a ***EMOTET***, seguir el siguiente enlace:

INFORMACIÓN SOBRE EMOTET