ENJOY SAFER TECHNOLOGY™

DÍA DEL CORREO

EL MAIL COMO VECTOR DE PROPAGACIÓN

En un mundo donde se envían **269 billones de mails por día** y **más de la mitad de la población mundial tiene al menos una cuenta de correo...***

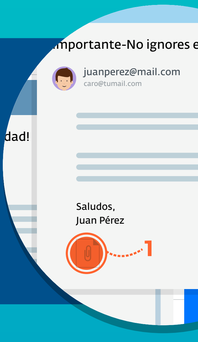
¿Qué amenazas se pueden desprender del correo electrónico?

RANSOMWARE

Modus operandi: llega como un adjunto para que el usuario ejecute o bien como un enlace a un sitio externo malicioso para que se infecte.

Funcionamiento: cifra archivos y los vuelve inaccesibles para el usuario.

¿Qué información afecta?: todos los archivos del equipo (y en ocasiones al equipo completo también).



PHISHING

Modus operandi: llega a nombre de una entidad legítima (como un banco o servicio online de alta reputación) que suele pedir las credenciales de acceso del usuario.

Funcionamiento: busca robar los datos como respuesta al correo o bien conducir a un sitio clonado de la entidad en cuestión.

¿Qué información afecta?: credenciales de acceso a sistemas.

Spear phishing: subcategoría del phishing que tiene el mismo fin y modus operandi, pero que no es masivo, sino que está dirigido a un perfil o a un objetivo específico que se quiere atacar.

Scam: subcategoría del phishing pero que implica una estafa monetaria, valiéndose de la ingeniería social para tentar a la víctima con una ganancia extraordinaria, como una lotería o una herencia, o apelando a lo emocional haciendo peticiones de ayuda caritativa a través de donativos.

SPAM

Modus operandi: el correo no deseado o basura se envía masiva y constantemente, generalmente a través de cuentas robadas o comprometidas.

Funcionamiento: distribuir publicidad no requerida, molestar, ocupar espacio en el correo, consumir recursos, colapsar servidores y propagar o distribuir malware.

¿Qué información afecta?: dependiendo del objetivo de la campaña de spam, puede afectar tanto al equipo y sus recursos, como también credenciales o información personal de la víctima.

BOTNET

Modus operandi: llega como un adjunto para que el usuario ejecute o bien como un enlace a un sitio externo malicioso para que se infecte.

Funcionamiento: convierte al equipo en un bot o zombi, de modo que el botmaster toma control del equipo de forma transparente al usuario.

¿Qué información afecta?: podría robar información, pero más allá de eso aprovecha los recursos del equipo para llevar a cabo actividades maliciosas como el envío de spam, la distribución de malware, el alojamiento de material ilegal o la realización de ataques de denegación de servicio distribuido.

* www.radicati.com/wp/wp-content/uploads/2017/01/Email-Statistics-Report-2017-2021-Executive-Summary.pdf