Caso de Ingeniería Social

Seguridad Informática

Juan Carlos Navidad García

Por alguna razón a una persona cualquiera se le ocurrió robarle la información a alguien famoso para venderla. Obviamente es un negocio redondo, pero bastante peligroso de ejecutar.

Bueno, esa persona, la cual información se desconoce, decidió robar información (fotos, vídeos, documentos) del móvil personal de Kim Kardashian.

¿Cómo lo hizo? Pensó en hacer un phishing, pero obviamente una persona famosa no sería tan insensata como para caer en eso. Estuvo pensando y pensando, así que se le ocurrió probar con ingeniería social, buscó por internet diferentes métodos para hacerse con toda la información posible y conocerla más profundamente, al igual que haría un gran fan de esa persona, indagar lo máximo posible tanto en su vida pública como privada.

Almacenó toda la información de su vida, de toda la información sacó muchísimas palabras clave que ella podría utilizar como clave de acceso, ya sean pines o contraseñas. Hizo un documento de texto con cada posible clave en una línea diferente, creando así un diccionario para sacar la contraseña a fuerza bruta.

Desarrolló un virus para poder acceder a distancia a su teléfono, pero para que ella se pudiese infectar, tenía que acercarse a su círculo, para ello pasó demasiado tiempo, se fue acercando poco a poco, en base a contactos fue consiguiendo el número de la asistenta de la agencia del representante, luego del secretario, representante y así hasta llegar a lo más cercano posible.

Se hizo pasar por un caza talentos de la televisión americana que necesitaba una nueva y famosa imagen para su programa, alguien que pudiese inspirar y llenar de ilusión a esas personas con talento sin recursos.

Gracias a eso consiguió su contacto, y mediante SMS y correo electrónico mandó un PDF infectado y prácticamente indetectable para cualquier antivirus, ese PDF contenía todo el supuesto proyecto e información.

Inocentemente ella picó y su teléfono fue infectado, pero obviamente iba a necesitar acceso para visualizar los datos que había en él. Después de los dos años investigando, el archivo de fuerza bruta tenía más de quinientas posibles claves y combinaciones.

Todo lo que pasó después ya se sabe, fue todo un éxito y a día de hoy se sigue sin saber quién fue…