Difusión: 52.645
Audiencia: 149.000

Expansión

13/02/04

UNIVERSO MULTIMEDIA

ENRIQUE DANS
Director del Área de Sistemas de Información del Instituto de Empresa

Las lecciones de los virus

Los piratas utilizan técnicas de ingeniería para penetrar en un sistema informático

El virus *MyDoom* ha infectado ordenadores de todo el mundo y ha provocado pérdidas millonarias. Nos ha llevado de nuevo a la época del salvaje Oeste con carteles que ofrecen recompensas a cambio de datos que permitan la captura del autor. Pero también ha resultado sumamente interesante al poner de manifiesto la importancia de una ciencia de la que cada vez vamos teniendo una información más completa: la ingeniería social.

En el mundo tecnológico, se conoce como ingeniería social a un tipo de técnicas utilizadas por los *hackers* o piratas informáticos para penetrar en un sistema de información. El *hacker* más famoso del mundo, Kevin Mitnick, era una persona calificada por sus compañeros de carrera como tecnológicamente muy deficiente. Sin embargo, era un maestro de la ingeniería social. ¿En qué consiste? Imagine que quiere usted acceder al ordenador de una gran empresa. Levanta el teléfono, llama a un trabajador de esa empresa, y le dice: "Fulanito, soy Manolo, de informática... ¿No has notado que la red te va últimamente muy lenta?" Seguro que hay algún Manolo en el Departamento de Informática de una gran empresa. Además, el riesgo es bajo: estoy al teléfono y, si Fulanito sospecha, puedo colgar. El siguiente paso se lo imaginan. Dado que todo el mundo opina que su red va más lenta de lo que debería ir, el *hacker*, con el pretexto de hacer unas pruebas, pide al usuario su contraseña y se despide educadamente. Las variaciones son infinitas y pueden incluir desde la simple mirada por encima del hombro cuando el usuario teclea su contraseña, técnica conocida como *shoulder surfing*, hasta la visita a la empresa, posiblemente vestido con un mono azul, que abre muchas puertas. Como puede verse, resulta de lo menos sofisticado tecnológicamente pero puede resultar devastadoramente efectivo.

En el caso de los virus, la cuestión toma derroteros muy similares. Virus enormemente eficaces fueron, por ejemplo, el *I love you* o *Kournikova*, que explotan una faceta muy concreta del ser humano que le lleva a abrir un fichero adjunto a un mensaje abandonando las precauciones que se supone debería tener. Nótese la habilidad del programador al escoger los temas. *I love you* llegaba a la bandeja de entrada desde el ordenador de alguien que te tenía en su libreta de direcciones y que aparentemente te confesaba su amor en un documento. Por eso, lo primero que se hacía era abrir el documento. *Kournikova* era aún menos sofisticado, ya que venía de un desconocido pero por alguna misteriosa razón el usuario también lo abría y, claro está, se infectaba.

MyDoom llega ya a un nivel de sofisticación de la ingeniería social francamente interesante: envía mensajes desde el ordenador de un usuario pero no con la dirección de ese usuario, sino con otras que obtiene mediante técnicas parecidas a los motores de *spam*. ¿El Resultado? Una serie de gente recibe un mensaje que le informa de que el mensaje que ha enviado a un usuario que normalmente desconoce ha resultado devuelto. Tras esto, el usuario intenta ver cuál es ese mensaje que no recuerda haber enviado. Revisa su bandeja de salida pero no encuentra nada. Por eso, existen grandes posibilidades de que abra el fichero adjunto para saber qué es eso que envió. El fichero, renombrado como un inofensivo *.txt*, no es tal fichero de texto sino un ejecutable con otra extensión oculta. En este caso, es la curiosidad y no el sexo la que lleva a abrir el fichero aunque al final el resultado es el mismo.

A pesar de esto, la ingeniería social también se puede aplicar para otros fines más honorables. En el universo digital las posibilidades de utilizarla para mejorar la respuesta a una campaña pueden resultar francamente interesantes. Démosle una vuelta. A lo mejor resulta que los virus también tienen lecciones que enseñarnos.

IV