VIRUS INFORMÁTICOS

28 de enero del 2008

SINOPSIS

Cada vez más nos vemos inmersos en un mundo virtual, pero no por ello menos real. Cada día, pasamos un montón de rato navegando por Internet, jugando con videojuegos o consultando el correo electrónico. Se trata del Ciberespacio, un entorno virtualmente infinito donde podemos hacer amigos, enviarnos fotos, ver videos o escuchar música. Sin embargo, como en el mundo real, acechan algunos peligros a la vuelta de la esquina (o de la página web). Son los virus informáticos, unas entidades que casi parecen dotadas de vida propia, y que pueden estropear nuestros archivos y nuestro disco duro en menos que hacemos un Reset.

QUEREMOS EXPLICAR

Qué son los virus informáticos y por qué se llaman así.

Las similitudes con los virus biológicos.

Los distintos tipos y los distintos niveles de peligro que conllevan.

Que los virus son creados por seres humanos.

Que tras el mundo cibernáutico hay personas con cara y ojos: hackers y crackers.

ÍTEMS PRINCIPALES

CLAVADITOS A SUS PRIMOS BIOLÓGICOS:

Los virus informáticos son programas informáticos muy pequeños pero con mucho poder, ya que pueden alterar el funcionamiento de un ordenador. En cierta manera, actúan como los virus biológicos, que son también partículas minúsculas que, cuando penetran en una célula, son capaces de destruirla. Además, tanto los virus biológicos como los informáticos tienen la capacidad de copiarse a sí mismos, es decir, de generar nuevos virus, exactamente iguales, que infectarán nuevas células u ordenadores.

En el caso de los virus biológicos, su mecanismo de acción suele ser introducirse en el ADN, que contiene las instrucciones para el correcto funcionamiento de la célula, y producir daños allí, de manera que la célula comienza a sufrir fallos y su orden interno se ve afectado. En el caso de los virus informáticos, su mecanismo de funcionamiento se basa en reemplazar archivos ejecutables por otros infectados con el código del virus.

UNOS GUSANOS MUY FECUNDOS:

Según la forma en que actúan, existen distintos tipos de virus. Los llamados *worms* (gusano en inglés) o gusanos se multiplican y ocupan la memoria, haciendo que el ordenador realice sus actividades de manera más lenta de lo habitual. Están diseñados, específicamente, para que puedan copiarse de un equipo al otro y son capaces de hacer muchísimas réplicas de sí mismo, sin necesidad de ir camuflados en un programa informático o archivo huésped. Por ejemplo, un gusano es capaz de enviar copias de sí mismo a todos los usuarios de una libreta de direcciones del correo electrónico, propagándose así muy rápidamente en una especie de efecto dominó. Esto hace que bloqueen redes

y que los usuarios vean cómo la navegación por Internet se hace mucho más lenta. Algunos crean una especie de “túnel” en el sistema, de manera que una persona ajena al ordenador infectado puede tomar control de la computadora de forma remota, apropiándose de ella.

NO TE PUEDES FIAR NI DE TU MAIL:

Los troyanos se llaman así en referencia al caballo de Troya mitológica, que se suponía que era un gigantesco regalo que hacían los griegos a los troyanos. En realidad, el enorme caballo de madera contenía en su interior a un montón de soldados griegos, que se escondían allí dentro con la intención de invadir la ciudad de Troya. De la misma manera, estos virus son programas informáticos que parecen ser software útil pero que esconden actividades dañinas para el ordenador. Por ejemplo, recientemente apareció un troyano que tenía la forma de un mensaje de correo electrónico que incluía archivos adjuntos que se suponía que eran actualizaciones de seguridad de Microsoft. Pues bien, en realidad estos adjuntos eran virus que deshabilitaban a los antivirus y, por tanto, permitían la entrada de un montón de programas que destruían el correcto funcionamiento del ordenador afectado. Este tipo de virus se difunden cuando los usuarios abren programas que creen que tienen orígenes legítimos.
A diferencia de los gusanos, no se propagan haciendo copias de sí mismos sino que infectan a otros ficheros. Por tanto, dependen de la actividad de los usuarios, es decir, de los humanos, para extenderse.

EL TÍPICO GRACIOSILLO:

Los *jokes* (broma en inglés) o virus broma crean mensajes jocosos en la pantalla y algunos son capaces de ejecutar el lector de CD o DVD abriéndolo y cerrándolo, o de controlar el ratón o el teclado. Su finalidad es, como bien dice su nombre, bromear con el usuario y no suelen ser destructivos, aunque sí son

molestos. Su objetivo es hacer creer al usuario que está siendo infectado por un virus peligroso. Pero al final todo se queda en un susto.

VIRUS QUE NO SON VIRUS:

Los *hoaxes* (hoax quiere decir engaño o broma pesada en inglés) o falsos virus, son mensajes con información falsa, que se suelen expandir a través del correo electrónico, con el objetivo de crear confusión entre los destinatarios o provocar una acción concreta de éstos que sea dañina para su ordenador. Por ejemplo, un mensaje del tipo “borre este archivo del equipo” puede provocar que los usuarios borren archivos del sistema necesarios para correcto funcionamiento de la computadora. Sin embargo, sólo pueden hacer daño si se les hace caso. Muchos de ellos tientan con la posibilidad de que te hagas millonario con sólo reenviar el mensaje o explican la historia de supuestos niños enfermos que necesitan tu ayuda, o repiten el esquema de las típicas cadenas de la suerte según las cuales hay que reenviar le mensaje so pena de sufrir una calamidad si cortas la cadena. En realidad, el objetivo de estos mensajes es conseguir direcciones de correo electrónico y congestionar los servidores.

Las cadenas de la suerte son algo muy típico. Unas fotos bonitas, a veces acompañadas con una música y unas frases bonitas que suelen terminar con algo como “manda este mensaje a 10 amigos y en una semana se cumpliran todos tus deseos”. En realidad, para la único que sirven es para conseguir direcciones de correo. Se puede hacer un símil, es como si encontrases tu número de teléfono publicado en el periódico o saliese por la tele. ¿Verdad que probablemente empezarías a recibir llamadas no solicitadas? Una recomendación: ¡rompe las cadenas! Pero si no lo quieres hacer, por lo menos borra todas las direcciones de correo que encuentres en el cuerpo del mensaje

y manda el mail con eso que se llama BCC (o copia oculta), de modo que el que lo recibe no podrá ver a quien más va dirigido este correo.

LA EPIDEMIA DEL SIGLO XXI:

La mayoría de infecciones las producen cada vez más los gusanos, que se transmiten a través de redes e Internet, y los troyanos, que suelen actuar a través del correo electrónico, ocultos en los archivos adjuntos o en la lectura de correos. Y no sólo los ordenadores son víctimas de estos virus. Ya están empezando a atacar a los teléfonos celulares, propagándose de móvil a móvil, y también a los asistentes digitales personales. La principal vía de contagio es el correo electrónico, que ya se puede consultar desde la telefonía móvil operativa. En un futuro, se cree que serán capaces incluso de grabar conversaciones y de enviarlas a través de la red o cambiar los números de las agendas, reemplazándolos con otros números de larga distancia, con el objetivo de generar enormes facturas de teléfono a fin de mes. La tendencia no es la producción de epidemias globales, como la que causó hace unos años el virus “I love you” sino las epidemias locales masivas en cortos periodos de tiempo.

Se ha llegado a punto de que uno se puede llegar a descargar un programa de Internet sin darse cuenta, pasando a formar parte de lo que se denominan “redes zombies”. Estos virus son ejecutados por control remoto por personas que hacen que el ordenador doméstico participe en actividades delictivas sin el permiso del dueño de la computadora.

¿CÓMO NOS PROTEGEMOS DE LOS VIRUS?

La mejor manera de prevenir una infección vírica es utilizando un antivirus. Son como las vacunas contra los virus biológicos. Un antivirus es un programa informático que rastrea las trazas que ha dejado un virus o software destructivo, detectándolo y lo eliminándolo, es como un perro sabueso virtual

Además de identificar al virus, muchos antivirus también pueden contener o parar las infecciones. Podemos concluir que son una especie de soldados centinela, que controlan las vías de entrada de las infecciones y que avisan de las incidencias al usuario del ordenador. Sin embargo, los nuevos virus que se crean cada año hacen que estos antivirus tengan que ser continuamente actualizados y mejorados para competir con las nuevas estrategias de invasión. Sin embargo, la potencia de un virus puede ser a veces difícilmente controlable. Por ejemplo, el gusano más rápido hasta la fecha, el Mydoom, afectó a 250.000 ordenadores en sólo un día en enero del 2004 y cinco años antes el Melissa obligó a los responsables de Microsoft, la empresa de informática más importante del mundo, a paralizar los sistemas de correo electrónico hasta que el brote epidémico estuviese completamente controlado.

Algunos consejos para estar protegido: no abrir archivos adjuntos si proceden de alguien que no conocemos. Aunque procedan de alguien conocido, intentar asegurarse que nos lo ha mandado de forma intencionada (si normalmente hablas en castellano con esa persona y el mail es en ingles… sospecha). Mantén actualizado tu antivirus, no descargues archivos de Internet si tienes dudas sobre su fiabilidad, etc. ¿Verdad que si vas de viaje a algún país exótico no te meterás a comer a un restaurante con una pinta horrible, con los manteles manchados y los platos sucios? Pues lo mismo pasa con las webs, si ves cosas raras, no te metas.

TRIBUS CIBERNÁUTICAS I: LOS HACKERS:

Además de los virus, existen otros peligros en el mundo de la informática. De hecho, en realidad, en última instancia los programas son ideados y diseñados por seres humanos, que son los que mueven las piezas del mundo virtual. Además de los propios programadores informáticos, han aparecido otras entidades alrededor de este ámbito desarrollándose colectivos como el de los

hackers. Los hackers son expertos en programaciones, redes computacionales y sistemas operativos, capaces no sólo de utilizarlos, sino de encontrar vías alternativas de modificación. El término *hacker* surgió del Instituto de Tecnología de Massachussets (MIT) en los años sesenta, para denominar a las personas que eran capaces de mejorar los programas y llevar a cabo cambios que nadie había podido hacer antes. Por otra parte, también se dice que la palabra deriva del verbo *to hack*, hachar en inglés, que es la acción que llevaban a cabo los técnicos en telefonía cuando arreglaban cajas defectuosas con un único golpe seco.

A pesar de la imagen que nos suelen mostrar los medios de comunicación, los hackers no son piratas informáticos. En realidad, los hackers proclaman que su interés en modificar software no se basa en ganar dinero sino en conseguir acabar con los monopolios de Microsoft y otras empresas que ganan muchísimo dinero gracias a los productos informáticos. Lo que los hackers quieren es democratizar el acceso a Internet y los diversos usos que esto deriva. Casi podríamos hacer una analogía entre los hackers, que serían como una especie de Robin Hoods que intentan devolver al usuario la autonomía y la libertad internáutica a través de intentar hacer daño a las grandes multinacionales, y sus primos segundos los crackers (de los que hablaremos en el siguiente apartado), que serían como los pícaros tunantes que intentan robarte la bolsa al menor descuido.

En este sentido, un sistema de software libre como Linux, que es gratuito y que compite con el coloso de Windows (de la empresa Microsoft) podría decirse que ha sido creado por hackers, en el buen sentido del término.

Hay una especie de “código de honor” entre los hacker. Por ejemplo, uno no se puede llamar a si mismo “hacker”, tienen que ser los miembros de la comunidad que le confieran esta distinción. También dicen cosas como:

- El mundo esta lleno de problemas fascinantes que hay que resolver

- Ningún problema debería tener que ser resuelto dos veces
- El aburrimiento y la rutina son nefastos
- Saber trucos de hacker no significa ser hacker. Un hacker crea, no copia.

TRIBUS CIBERNÁUTICAS II: LOS CRACKERS:

Los crackers son personas que violan la seguridad de los sistemas informáticos y, a diferencia de los hackers, intentan beneficiarse personalmente o hacer daño con su acción. Suelen romper los códigos que permiten acceder a los programas sólo a aquellos que han pagado un dinero por ellos, por ejemplo. El término proviene de la unión de la expresión *Criminal hacker*, creada en 1985 en contraposición al término *hacker*, para defender la respetabilidad de éstos últimos.

En cierta manera, podemos decir que los hackers temen a los crackers, que son los que dan mal nombre a los primeros. Algunos crackers han llegado a penetrar hasta en los ordenadores del FBI y el ejército americano.

Por otra parte, los crackers son también personas que diseñan o programan cracks informáticos, que modifican las funciones del software original, dándole nuevas utilidades. En este caso, podríamos decir que estos crackers "benignos" lo que hacen es "tunear" los programas informáticos para que sean más completos, mejorando sus prestaciones.

ÍTEMS SECUNDARIOS

LOS PRIMEROS VIRUS INFORMÁTICOS:

El primer ataque vírico se produjo en 1972 y la víctima fue un ordenador IBM. Este primer virus era un programa bastante inofensivo, que simplemente producía este mensaje de manera periódica en la pantalla de la computadora: “Soy una enredadera, agárreme si puedes”. Enredadera, en inglés, se llama *Creeper*, así que éste fue su nombre. Naturalmente, no surgió de la nada sino que fue diseñado por un hombre y, en principio, era incapaz de replicarse en otro ordenador. Con la intención de eliminarlo, también fue diseñado el primer programa antivirus, llamado *Reaper*, segadora en inglés.

Diez años más tarde, apareció el primer virus capaz de replicarse en distintos ordenadores. Esta vez si que fue un accidente. Mientras que la función inicial del programa, al que llamaron premonitoriamente “gusano”, era hacer copias de seguridad mientras pasaba de una a otra computadora de las instalaciones, en la práctica el gusano fue capaz de llegar hasta ordenadores fuera del laboratorio y se extendió por toda la red, paralizando las máquinas. A pesar de que se intentó eliminar, continuó apareciendo y tuvieron que crear otro programa, capaz de extenderse de la misma manera, que fuese destruyendo las copias del gusano. A partir de finales de los años ochenta, comenzaron a aparecer virus creados por personas, en el anonimato, que infectaban universidades u oficinas y originaban grandes destrozos.

EL FAMOSO SPAM:

En realidad, el Spam es un jamón con especias (*Spiced Ham*, en inglés, cuya abreviatura es Spam) que se comenzó a producir en 1926 y que constituía el primer producto de carne en lata que no necesitaba refrigeración. Por tanto, se expandió por todas partes y tanto los americanos como los rusos lo utilizaron para el consumo de sus tropas durante la Segunda Guerra Mundial. Debido a

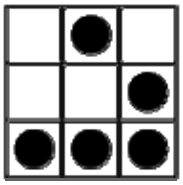
su ubicuidad, se ha llamado precisamente así la presencia del correo electrónico no deseado, que también está por todas partes. De hecho, el spam se ha convertido en una de las cosas más odiadas de Internet.

SIMILITUDES SORPRENDENTES:

Algunos virus no son muy dañinos y sólo se propagan y se replican, pero otros llegan a destruir todos los datos almacenados en un ordenador o a bloquear redes informáticas. Existen virus biológicos que actúan directamente, justo cuando infectan una célula, y otros que se esconden en el ADN y tardan mucho tiempo en manifestarse. Con los virus informáticos pasa igual: algunos infectan a los programas en el momento en que se ejecutan, y otros, en cambio, son virus residentes, es decir, que se instalan en la memoria RAM de la computadora. De esta manera, el virus toma el control de los sistemas básicos del sistema operativo infectando después todos los archivos a medida que se vayan ejecutando, poco a poco.

Y las similitudes no se quedan aquí. Ambos tipos de virus se reproducen de manera exponencial y pueden resultar típicos de distintos lugares geográficos. De la misma manera que un virus biológico como el de la gripe del pollo tiene su origen en Asia, en Europa y EEUU son más comunes los virus informáticos tipo troyanos espías, en Latinoamérica los troyanos bancarios, y en la región asiática los troyanos especialistas en juegos en línea y los gusanos. También existen determinadas épocas del año en que los virus tienen mayor actividad. Igual que el virus de la gripe suele causar estragos en invierno debido a las bajas temperaturas, muchos virus informáticos se expanden más rápidamente en Navidades, ya que se camuflan en las postales y felicitaciones que la gente se manda mediante el correo electrónico durante esas fechas.

INFORMACIÓN ADICIONAL

	El glider, símbolo del hacker.

LINKS DE INTERÉS

http://www.howstuffworks.com/virus.htm

http://www.vmyths.com/