Anexo V

Historia de los virus informáticos

Álvaro Gómez Vieites

ANEXO V

HISTORIA DE LOS VIRUS INFORMÁTICOS

Podemos distinguir cuatro generaciones de virus informáticos:

- Virus de ordenador personal que infectan a ficheros ejecutables y sectores de arranque.

- Virus de macro, capaces de infectar a documentos que soportan lenguajes de macros.

- Virus que tienen capacidad para propagarse a través de redes como Internet ("gusanos"), mediante el correo electrónico, servidores conectados a la Red, aplicaciones P2P, clientes IRC, etc.

- Virus que pueden afectar a otro tipo de dispositivos: teléfonos móviles, agendas electrónicas, electrodomésticos, etc.

La primera referencia sobre los virus data de 1949, cuando el matemático John von Neuman mencionó el concepto de virus informático en su artículo "*Theory and Organization of Complicated Automata*".

En la década de los sesenta en los laboratorios Bell se desarrollaron juegos (programas informáticos) que eran capaces de luchar entre sí con el objetivo de acaparar el mayor espacio de memoria posible del sistema informático donde se ejecutaban. Estos programas, conocidos como "Core Wars", desarrollaron técnicas de

ataque, defensa, ocultamiento y reproducción que posteriormente adoptaron los virus informáticos.

Posteriormente, en 1970 John Shoch y Jon Hupp crearon en el Centro de Investigación de Palo Alto (PARC –*Palo Alto Research Center*–) de Xerox programas autorreplicables que permitían controlar la salud de las redes informáticas. Uno de ellos se denominó "el gusano vampiro", porque se "escondía" en la red y se activaba por las noches. No obstante, días después de haber sido instalado, este gusano se propagó por todas las máquinas de la red del PARC, reproduciéndose hasta tal punto que llegó a colapsar completamente la red y todos los ordenadores conectados. Para eliminar este gusano tuvieron que elaborar otro programa, que podría considerarse como el precursor de los antivirus actuales.

El 10 de noviembre de 1983 el estudiante de doctorado estadounidense Fred Cohen presentó el que actualmente se considera como el primer virus informático de la historia. El propio Cohen describió su programa como un virus capaz de "infectar" a otros programas, incluyendo en los mismos una versión idéntica de sí mismo.

También en 1983, Ken Thompson daba a conocer las "Core Wars", animando a la experimentación con esas pequeñas "criaturas lógicas", noticia que era difundida por la revista *Scientific American*.

En el año 1985 aparecieron los primeros virus para el sistema MS-DOS, que se propagaban a través de disquetes. Finalmente, en el año 1987 se desarrollaron los primeros virus informáticos y otros programas dañinos de gran difusión. Los primeros antivirus comerciales se presentaron al año siguiente, en 1998. Surge entonces la *Computer Virus Industry Association* (Asociación de la Industria de los Virus Informáticos) en Estados Unidos, iniciándose una labor de concienciación sobre la necesidad de defender los sistemas informáticos de los ataques desencadenados por los virus y otros programas dañinos.

Seguidamente se presenta una relación cronológica de algunos de los virus informáticos más famosos, describiendo sus características más innovadoras y sus posibles consecuencias para los sistemas infectados:

- "Brain" (1986): considerado como el primer virus informático difundido fuera de un laboratorio o centro de investigación. Desarrollado en Pakistán, infectaba el sector de arranque de los disquetes, utilizando técnicas de enmascaramiento para conseguir que el ordenador no se percatara de su presencia. Fue el primer virus reseñado en los medios de comunicación (revista *Time Magazine*).

- "Stoned" (1987): otro virus de los pioneros, que infectaba el sector de arranque del disco duro del ordenador.

- "Jerusalem" (1987): también conocido como "Viernes 13", porque los efectos dañinos del virus se desencadenaban en esa fecha. Fue descubierto

a finales de 1987 en la Universidad Hebrea de Jerusalén, siendo uno de los primeros en infectar ficheros, borrándolos cuando se ejecutaba. Se trata de uno de los virus más famosos de la historia, debido a su técnica de programación (primero en quedar residente en el sistema) y a que a partir de él se crearon numerosas variantes.

- "Gusano de Morris" (1988): el 2 de noviembre de 1988 Internet, entonces aún llamada ARPANET, sufrió un grave ataque que provocó que toda la red se colapsara a causa de un "gusano" que consumía la memoria de los ordenadores conectados a la red y ralentizaba su funcionamiento. Las copias del gusano se difundían a través del correo electrónico, gracias a una vulnerabilidad del servidor de correo Sendmail de UNIX, consiguiendo infectar en unas pocas horas a los ordenadores de un gran número de universidades y de importantes instituciones científicas como la NASA, el laboratorio de Inteligencia Artificial del MIT (*Massachusetts Institute of Technology*), la red del Departamento de Defensa norteamericano (MILNET), etc.

Figura 1: Robert Morris

Se estima que el coste de este incidente, debido al colapso provocado en numerosos servidores que estaban conectados a Internet, sobrepasó el millón de dólares. Afortunadamente, este gusano no provocaba daños en los datos y ficheros almacenados en los servidores. Su creador, Robert Morris Jr., un graduado de Harvard de 23 años que reconoció su error y lo calificó de "fallo catastrófico", fue finalmente detenido y condenado por la Justicia de Estados Unidos.

- "Dark Avenger" (1990): inicia una nueva generación de virus procedentes sobre todo de Bulgaria.

- En 1991 se dan a conocer las primeras herramientas que facilitan la creación de virus, entre las que podríamos citar "Virus Creation Laboratory", "Phalcon/Skism Mass-Produced Code Generator", etc.

- "Michelangelo" (1992): virus que infectaba el sector de arranque de los disquetes y el registro maestro de arranque (MBR) de los primeros discos

duros, y actuaba el día 6 de marzo, coincidiendo con el aniversario del nacimiento del famoso escultor y pintor Miguel Ángel.

- "Concept" (1995): primer virus de macro. Aprovechaba el lenguaje de macros desarrollado por Microsoft para automatizar tareas en las distintas herramientas de Office, para infectar los documentos de los usuarios del equipo infectado.

- "Laroux" (1998) y "AccessiV" (1998): primeros virus de macro para Excel y Access, respectivamente.

- "Strange Brew" (1998): primer virus desarrollado en el lenguaje Java.

- "Chernobyl" o "CIH" (1999): virus que formateaba el disco duro y que podía ocasionar daños en el propio hardware del ordenador infectado, ya que estaba programado para reescribir la memoria Flash BIOS del equipo, con lo cual éste no era capaz de arrancar y quedaba inservible, siendo necesario avisar al servicio técnico para su recuperación. La única solución consistía en reemplazar la BIOS o la placa base, con el coste y la pérdida de tiempo que ello significaba.

- "Funlove" (1999): primer gran virus de red, que todavía se encuentra activo a día de hoy, provocando infecciones en redes empresariales.

- "Happy99" (1999): gusano de correo electrónico que adquirió una cierta notoriedad a principios del año 1999.

- "Melissa" (marzo de 1999): este virus consiguió infectar 4 millones de ordenadores en tan sólo 3 días, utilizando un mecanismo exponencial de propagación a través del correo electrónico. Cada ordenador infectado intentaba infectar 50 nuevos ordenadores obtenidos de la libreta de direcciones del programa lector de correo.

- "I-Worm.ExploreZip" (junio de 1999): otro peligroso gusano de correo electrónico que en pocos días consiguió infectar numerosas redes corporativas y miles de ordenadores en todo el mundo. La infección se inició en los grupos de noticias, donde el autor del gusano publicó un mensaje con una copia incluida de éste.

- "VBS/Loveletter", alias "I_Love_You" (mayo de 2000): primer gusano de correo electrónico escrito en el lenguaje VBScript. De hecho, hasta su aparición los "*scripts*" ejecutables de Windows habían pasado inadvertidos para los expertos en seguridad. El virus de la "carta del amor" ("*Love Letter*") infectó a 40 millones de ordenadores en tan sólo 6 horas, utilizando un mecanismo exponencial de propagación a través del correo electrónico, ya que cada ordenador infectado intentaba infectar

todas las direcciones de la libreta de direcciones del lector de correo electrónico.

- "VBS/Timofonica" (junio de 2000): virus de origen español realizado en VBScript y que, al igual que el virus "I_Love_You", utilizaba la libreta de direcciones del lector de correo para reenviarse a todas las direcciones que se encontraban en ella. Una vez ejecutado, el virus enviaba un mensaje a móviles de la operadora española Telefónica, cuyo número generaba de manera aleatoria, utilizando para ello la dirección "correo.movistar.net".

- "Nimda" (septiembre 2001): virus de Win32 que utilizaba distintos mecanismos de propagación, explotando varias vulnerabilidades presentes en servidores Web y en los navegadores:

    - Infección a través del correo electrónico aprovechando la vulnerabilidad "IFRAME"[1] de Internet Explorer para conseguir ejecutarse e infectar de forma automática a un equipo, con tan sólo visualizar un mensaje infectado, sin necesidad de que el usuario abra el archivo que contiene el virus. El mensaje de correo en cuestión incluía como adjunto un fichero denominado "readme.exe" con el código vírico. Se trata, además, de uno de los primeros virus que contiene su propio motor SMTP, de forma que no necesita que el usuario tenga configurado un servidor de correo para poder reenviarse a otros usuarios.

    - Infección a través del navegador, al visualizar una página Web de un servidor infectado. La página Web contiene un código en el lenguaje Java Script que intenta abrir el fichero de correo "readme.eml", que incluye el fichero adjunto con el virus:

        ```
        <html><script language="Java Script">
        window.open("readme.eml") </script></html>
        ```

    - Infección a través de la propia red local: Nimda podía recorrer todas las unidades locales y de red e infectar todos los directorios a los que lograba tener acceso (infección a través de recursos compartidos mediante el protocolo NETBIOS de las redes Windows), creando múltiples archivos de mensajes de correo electrónico (.eml) con nombres aleatorios, y modificando los ficheros de extensión .HTML, .HTM o .ASP para que al abrirlos se ejecutase de forma automática el fichero "readme.eml" y se produjera en ese momento la infección del equipo.

[1] Los detalles de esta vulnerabilidad habían sido publicados en marzo de 2001.

- Infección de servidores Web explotando la vulnerabilidad conocida como "*Web Server Folder Traversal*", que permitía ejecutar código en los servidores Internet Information Server a través de una determinada petición Web maliciosa[2]. Microsoft ya había publicado el parche de esta vulnerabilidad en octubre de 2000 y, sin embargo, muchos servidores Web no habían sido actualizados correctamente por sus administradores, facilitando de este modo la propagación del nuevo virus. En un servidor Web vulnerable Nimda trataba de ejecutar una sesión TFTP y descargar en un directorio del servidor el archivo "ADMIN.DLL", que contenía el código vírico para tomar el control de la máquina.

- La estimación de los daños provocados por el virus "Nimda" supera los 500 millones de dólares.

- "SirCam" (2001): otro famoso virus desarrollado en el año 2001.

- "CodeRed", "CodeRed II", "CodeBlue" (2001): primeros virus con capacidad de propagación mediante el protocolo HTTP, a través de servidores Web con un agujero de seguridad (se trataba nuevamente del servidor Internet Information Server de Microsoft). La estimación de los daños provocados por estos virus supera ya los 2.500 millones de dólares.

- "BadTrans.B" (noviembre 2001): otro famoso virus desarrollado en el año 2001.

- "Klez" (abril 2002): se trata de uno de los virus más persistentes de todos los tiempos, que emplea distintos métodos de propagación. Así, los virus "Nimda", "BadTrans", "Klez" y otros similares explotaban una debilidad del formato MIME del correo electrónico, modificando la cabecera de los mensajes de correo para hacer referencia a un formato de fichero adjunto confiable para el sistema, consiguiendo de este modo que éste "bajase la guardia" y tratase de ejecutar el contenido adjunto a un mensaje de correo electrónico, sin comprobar si se trataba de un fichero del formato indicado en la cabecera del correo:

  - En el caso del virus "BadTrans", la modificación realizada en la cabecera del mensaje de correo era la siguiente:

    Content-Type: audio/x-wav; name="news_doc.DOC.scr" (el virus trataba de simular que el contenido adjunto se correspondía con un fichero de audio).

[2] Se trataba de una petición GET vía HTTP que trataba de tener acceso al intérprete de comandos del sistema: "CMD.EXE".

- En el caso del virus "Nimda", la modificación realizada en la cabecera del mensaje de correo era la siguiente:

  Content-Type: audio/x-wav; name="readme.exe" (el virus trataba de simular que el contenido adjunto se correspondía con un fichero de audio).

- En el caso del virus "Nimda", la modificación realizada en la cabecera del mensaje de correo era la siguiente:

  Content-Type: audio/x-wav; name=200).exe (el virus trataba de simular que el contenido adjunto se correspondía con un fichero de audio).

- Hay que tener en cuenta que los lectores de correo Outlook y Outlook Express de Microsoft utilizan el navegador Internet Explorer para interpretar los mensajes en formato HTML. El navegador abría de forma automática el archivo adjunto en el correo, al creer que se trataba de un archivo de sonido aparentemente inofensivo para el sistema.

- "Bugbear" (2002): virus similar al "Klez", ya que también aprovechaba la vulnerabilidad "IFRAME". Se replicaba a través del correo electrónico y mediante unidades compartidas de red, siendo capaz de detener los procesos de los programas antivirus y cortafuegos instalados en la máquina infectada. Además, se encargaba de capturar todas las pulsaciones del teclado y abría una puerta trasera en el equipo infectado que permitía el acceso y control indiscriminado de forma remota. "Bugbear.B" es una variante surgida en el año 2003.

- "SQL Slammer" (2003): se trata del virus más novedoso del año 2003, tanto por su técnica de programación como por atacar a sistemas tan críticos para las empresas como son sus bases de datos. Se propagó utilizando una vulnerabilidad del sistema gestor de bases de datos SQL Server de Microsoft. Su rapidez de propagación llegó a colapsar todas las redes infectadas (se estima que en tan sólo 10 minutos consiguió recorrer todo el mundo, dificultando de este modo su contención).

- "Blaster", "SoBig" y "Mimail" (agosto 2003): otros virus famosos del año 2003.

- "MyDoom" (enero 2004): virus que nuevamente bate récords de propagación, abriendo puertas traseras en los equipos infectados y facilitando el control remoto de estos equipos. Además, lanza ataques dirigidos desde los equipos infectados contra los Websites de las empresas SCO y Microsoft (ataques de Denegación de Servicio para tratar de bloquear el funcionamiento de estos Websites).

- "Sasser" (mayo 2004): gusano que aprovecha un desbordamiento de "*buffer*" en el servicio LSASS de los sistemas Windows, para infectar de forma automática a otros sistemas que se encontraban conectados a la red, utilizando una conexión a través del puerto TCP/445. Una vez que tomaba el control, dejaba instalada una "puerta trasera" en el equipo infectado que posibilitaba la posterior intrusión de atacantes remotos. "Sasser" podía infectar todos los sistemas Windows 2000 y Windows XP que no habían aplicado el parche de seguridad "MS04-0112" que Microsoft distribuyó en abril de 2004.

    - La propagación de "Sasser" a través de Internet fue exponencial, al realizar un barrido de direcciones IP semialeatorio desde los equipos ya infectados. Cada vez que conseguía contactar con el puerto TCP/445 en alguna de las direcciones IP escaneadas, enviaba el código para explotar la vulnerabilidad LSASS, de forma que si el sistema era vulnerable lograba abrir un intérprete de comandos ("shell") en el puerto TCP/9996. Desde ese intérprete de comandos forzaba una conexión al puerto TCP/5554 del ordenador infectado desde el que había realizado el barrido de direcciones IP, para descargar por FTP el ejecutable del gusano.

    - Además de provocar una ralentización general del equipo debido a todos los procesos que lanzaba el gusano para realizar los barridos de direcciones IP, la explotación del desbordamiento de "*buffer*" del servicio LSASS mostraba mensajes de error en el equipo y forzaba el reinicio del sistema, volviéndolo totalmente inoperativo.

- "Bagle" (octubre y noviembre 2004): gusano capaz de detener la ejecución de varios procesos, entre ellos algunos asociados a herramientas de seguridad informática (como los antivirus y los cortafuegos). Además, abría una puerta trasera (en el puerto TCP 81) en el equipo infectado, facilitando de este modo el acceso no autorizado por parte de otros usuarios remotos conectados a través de Internet.

- "Zafi.D" (diciembre de 2004): nuevo gusano que se propagaba a través de redes "*peer-to-peer*" y mensajes de correo electrónico. Aprovechó las fechas navideñas para propagarse rápidamente mediante falsos mensajes de felicitación.

- "Skulls" (diciembre de 2004): uno de los primeros códigos malignos para teléfonos móviles, presentando además características de troyano, ya que se incrustaba en programas "*freeware*", como las melodías o los protectores de pantalla para el teléfono. Infectaba al sistema con el gusano "Cabir.B" (el primer gusano para móviles), que se podía propagar a través de conexiones Bluetooth y afectar a otros teléfonos próximos. Sólo resultaban vulnerables los teléfonos móviles con el sistema operativo

Symbian. Al ejecutarse deshabilitaba casi todas las funciones del teléfono, convirtiendo los iconos en calaveras y mostrando un mensaje al usuario en la pantalla del terminal infectado.

- "Santy" y variantes (diciembre de 2004): gusano que se propagaba a través de los servidores Web PHP[3] que contenían ciertos errores de programación, al no filtrar de forma adecuada los parámetros de entrada de determinadas funciones. Este gusano trataba de localizar los servidores Web potencialmente vulnerables a través de motores de búsqueda como Google o Yahoo!. Para ello, analizaba sintácticamente las direcciones URL de las páginas Web que eran ofrecidas por uno de estos servidores, sobrescribiendo las variables con cadenas para aprovecharse de la posibilidad de incluir código dañino que sería ejecutado por el servidor. Cuando tenía éxito, el gusano podía descargar y ejecutar un programa o un "*script*" en el servidor vulnerable.

- "Commwarrior.A" (marzo 2005) y "Mabir.A" (abril de 2005): nuevos gusanos que atacaban a los teléfonos móviles con el sistema operativo Symbian. Se propagaban mediante respuestas a mensajes de texto (SMS) o multimedia (MMS), así como a través de conexiones Bluetooth. De este modo, sus consecuencias para la víctima eran un incremento en la factura del teléfono (por el envío de los mensajes a móviles) y una descarga más rápida de la batería del terminal (debido a las conexiones Bluetooth).

- "PGPCoder" (mayo 2005): troyano que cifraba los archivos de extensiones .xls, .doc, .txt, .rtf, .zip, .rar, .dbf, .htm, .html, .jpg, .db, .db1, .db2, .asc y .pgp en el sistema infectado, dejando a continuación un mensaje solicitando dinero a los usuarios afectados si querían volver a restaurar sus ficheros (mediante el envío de una clave para descifrarlos).

Podemos apreciar en esta revisión cronológica de los virus y otros programas dañinos cómo han ido refinando sus técnicas de propagación en estos últimos años, explotando en muchos casos varias alternativas a la vez. Por este motivo, su rapidez de propagación se ha incrementado de forma espectacular, de tal modo que hoy en día en apenas unos minutos un nuevo "gusano" podría afectar a cientos de miles de equipos conectados a Internet, ocasionado importantes pérdidas económicas a las organizaciones afectadas.

También conviene destacar que en la mayoría de los casos los virus han aprovechado vulnerabilidades de navegadores, sistemas operativos, servidores u otras aplicaciones informáticas para propagarse.

---

[3] PHP es un lenguaje de "*scripting*" de propósito general, utilizado para crear páginas HTML dinámicas en un servidor Web.

De ahí la importancia cada vez mayor de actualizar de forma correcta y rápida los sistemas informáticos, utilizando los parches publicados por los fabricantes de software y los servicios de actualización automática, como WindowsUpdate de Microsoft.