HISTORIA DE LOS VIRUS

Alianza por la SEGURIDAD en internet

TECNOLOGIA EXPLICADA:
Cronología de hechos relevantes sobre los Virus

1949

El científico húngaro **John Louis Von Neumann** publica en articulo 'Theory and Organization of Complicated Automata', donde demostró la posibilidad de crear programas que pudieran tomar el control de otros. (algunos autores citan esta publicación en 1939)
Inspirados en esta teoría, 3 jóvenes de la Bell Computer crearon un juego llamado **CoreWar** para su propio entretenimiento, consistente en invadir la computadora del adversario consumiendo la memoria de sus oponentes, ganando el que finalmente eliminara los programas de sus adversarios.

1950 a 1980

Aunque mantenidas en la clandestinidad por muchos años, se conocen diferentes historias de auténticas muestras de intelectualidad como el virus 'Creeper' (enredadera), que se 'arrastraba' por las redes presentando el mensaje 'Soy la enredadera, atrápame si puedes', y lo que podría llamarse el primer anti-virus, llamado 'Reaper' (segadora) que servia para deshacerse de él

1981

IBM lanza la IBM PC, y la prisa por salir al mercado impidió que se le diseñara un buen sistema operativo. La versión del PC-DOS basado en el MS-DOS adquirido a Microsoft estaba plagado de fallas que lo hacían en verdad vulnerable a los virus.

1982

Se creó un virus para Apple II diseñado para viajar por toda la red, denominado por su autor Jim Hauser, como "viajero electrónico" (Electronic hitchhicker) que se pegaba a programas sin ser detectado.

1983

Ken Thompson, creador en 1969 del UNIX demostró la forma en que se podía crear un virus informático. El Dr. Thompson, en una intervención en la Association for Computing Machinery, da a conocer la existencia del programa CoreWar, con detalles acerca de su estructura. La revista Scientific American lo publica en su artículo "Computer Recreations" en el numero de mayo de 1984 ofreciendo por 2 dólares al público las guías para la creación de sus propios virus.

1984

El **Dr. Fred Cohen** es homenajeado en su graduación del doctorado en Ingeniería Eléctrica en la que presenta formalmente las pautas para la creación de un virus. Es reconocido como el padre de los virus pues se trata del primer autor que abiertamente publica información al respecto. Ese mismo año escribe su libro 'Virus informáticos: Teoría y experimentos'.

Sin embargo, la primera gran alarma se dio en un foro de debates de lo que después se convirtió en la revista BYTE, cuando los usuarios reportaron la propagación de programas que habían llegado a sus computadoras en forma repentina actuando como 'caballos de troya', es decir, ocultos en otros programas.

1986

Aparece el virus © **Brain, atribuido a dos hermanos paquistaníes**, quienes desarrollaron este código para evitar que la gente copiara los programas que fabricaban. Si alguien lo hacía, el © Brain castigaba al pirata invadiendo todo su disco duro y borrando los programas.

1988

Robert T. Morris difunde un virus en **ArpaNet**, una de las redes precursoras de Internet, logrando infectar a 6000 servidores. Cabe mencionar que ArpaNet utilizaba el sistema operativo UNIX. Morris fue descubierto, enjuiciado y condenado a 4 años de cárcel y $10,000 dólares de multa, hecho que finco un precedente y desalentó a otros programadores con intenciones nocivas.

1989

Aparece el virus **Dark Avenger**, uno de los primeros virus hechos en Bulgaria y uno de los más destructivos y del cual se han escrito varios libros. Se hizo terriblemente famoso por su ingeniosa programación y peligrosa y rápida técnica de infección.

Un "Caballo de Troya" se distribuyo en 10.000 copias de un paquete con información sobre el SIDA. El programa, de una empresa panameña llamada PC Cybort, encriptaba el contenido del disco duro y pedía al usuario que pagara por la licencia de uso para obtener la clave de desencriptación.
Se detecto el virus **Datacrime**, el cual fue erróneamente llamado Columbus day virus (virus del día de Colón) porque se suponía que se activaría el 12 de octubre, pero realmente se activaba después de ese día (del 13 de octubre al 31 de diciembre). Causo una reacción desmedida entre la gente por la información errónea en revistas y periódicos. Kenneth R. Van Wyk, moderador de VIRUS-List, comento sobre el asunto "El pánico parece ser más destructivo que cualquier virus por sí mismo"

Y el 23 de Marzo de 1989, un virus ataca sistemas informáticos de hospitales, variando la lectura de informes de laboratorio.

1992

Aparece el virus **Michelangelo** por primera vez. Es el virus que más publicidad ha recibido y gracias a él se tuvo más conciencia de la peligrosidad de los virus, ya que se difundió la alerta de que más de 5 millones de PCs podían quedar inoperantes el 6 de marzo de este año.

1994

El virus **Natas** inicio una "epidemia" por todo México. Se cree que es de origen mexicano.

1995

A mediados de 1995 se reportaron en diversas ciudades del mundo la aparición de una nueva familia de virus que no solamente infectaban documentos, sino que a su vez, sin ser archivos ejecutables podían auto-copiarse infectando a otros documentos. Los llamados **'macro virus'** tan sólo infectaban a los archivos de MS-Word, posteriormente apareció una especie que atacaba a otros procesadores de textos. En 1997 se disemina a través de Internet el primer macro virus que infecta hojas de cálculo de Excel, denominado **Laroux**, y en 1998 surge otra especie de esta misma familia de virus que ataca a los archivos de bases de datos de MS-Access.

1999

Aparecen los virus en archivos adjuntos en mensajes de correo electrónico, como el **Melissa**, el CIH y el ExploreZip. A finales de Noviembre aparece el famoso **BubbleBoy**, primer virus que infecta los equipos con solo leer el mensaje de correo escrito en lenguaje HTML. Este peligroso virus explotaba una vulnerabilidad del Sistema Operativo, lo que permitió elevar la conciencia de los usuarios sobre la importancia de mantener actualizado su software.

Cabe mencionar que el virus Melisa no causaba daño a las computadoras infectadas, pero si a la infraestructura de Internet, ya que ocasionaba un excesivo trafico de mensajes de correo auto-enviados desde todas las PCs atacadas. Cadenas de TV anunciaron que el virus estaba paralizando los servidores de correo de importantes empresas como Microsoft e Intel, quienes se vieron obligados a inhabilitar sus redes por muchas horas. El FBI hizo la promesa (y la cumplió) de llevar ante la justicia al autor del virus. El sitio Web del primer proveedor de anti-virus en ofrecer una vacuna recibía 10,000 visitas diarias. Según IDC, las pérdidas provocadas por virus entre marzo y junio de 1999 ascendieron a 7,200 millones de dólares.

Es válido decir que a partir de este año, los virus informáticos se hayan convertido en el mayor problema de seguridad para los responsables de las áreas de sistemas.

2000 a 2003

Aparecieron innumerables instancias de virus que se auto-envían adjuntos en correos electrónicos, como el **CodeRed**, el **Netsky**, el Beagle y el Nimda. Los costos de reparación en empresas por ataques de virus alcanzan niveles estratosféricos. Virus como el **Blaster** demuestran que los costos por pérdida de productividad también pueden ser muy altos, ya que paralizan la actividad de las redes de las personas y los negocios. Los virus perfeccionan su capacidad de polimorfismo y mutación.

2004

En enero de este año aparece el virus **MyDoom**, que viene a demostrar que un anti-virus ya no es suficiente para garantizar la seguridad de un equipo, ya que demuestra la capacidad de abrir las llamadas 'puertas traseras' (backdoors) y utilizar su propio sistema de envío masivo de correos para propagarse, saturando y colapsando la infraestructura de Internet. Es por este motivo que independientemente de lo importante que es contar con una solución antivirus, los otros pasos de seguridad básica son igualmente fundamentales para su equipo hoy en día: Mantener al día su sistema operativo y utilizar un Firewall que impida el uso de puertas no autorizadas.

Este año se caracteriza por la extensa aparición de variantes de un mismo virus, ya que se crea como moda que los programadores malintencionados publiquen sus códigos en sitios web abiertos para que otros programadores los puedan fácilmente reproducir.

2005

La producción de virus hoy en día avanza a razón de 40 nuevos virus diarios.

Otros números interesantes:

Se estima que a la fecha, los productos anti-virus detectan alrededor de 70,600 virus.

En el 2002, uno de cada 212 correos contenía un virus, en el 2003 uno de cada 33 y en el 2004 uno de cada 16, se estima que al final del 2005 uno de cada 12 mensajes estará contaminado.

Además, sigue la tendencia de los últimos meses, y los virus tal como los conocemos dejan su lugar a los códigos Troyanos y a los Gusanos, capaces de construir redes de bots para propósitos ilegales como robar dinero o "tirar" servidores web.

2006

Empiezan a tomar popularidad los juegos en línea como SecondLife, World of WarCraft, etc… lo que da lugar a la aparición de código malicioso para robar nombres de usuario y contraseñas de estos sitios.

Los ataques de Phishing ya se convierten en algo cotidiano, y por el alertamiento masivo a usuarios de banca electrónica para no responderlos, su efectividad se reduce. Esto da lugar a la aparición del troyano **Qhost**, capaz de modificar el contenido del archivo Hosts en equipos Windows con la intención de redirigir al usuario a páginas web falsas, con lo que inicia masivamente el nuevo fenómeno llamado **Pharming.**

Por el daño patrimonial que ya causan el malware, las autoridades en todo el mundo ya persiguen más intensamente a los delincuentes detrás de ellos. En Marruecos, dos estudiantes creadores del gusano **Zotob** son enviados a prisión.

Aparece también el gusano Stardust, capaz de infectar macros de OpenOffice, al igual que el Leap, capaz de atacar el Mac OS X, propagándose a través de iChat.

Otros troyanos importantes de este año: **HaxDoor, IRCBbot y el Spamta**.

2007

Las organizaciones delictivas cada vez adoptan con más fuerza el uso de internet para sus propósitos. Se atribuye a la organización Russian Bussiness Network el haber modificado la página del Banco de la India para que cada visitante fuera automáticamente infectado por un código capaz de revelar su información confidencial.

Crece el uso de código que incluye Keyloggers como adjunto en correos de Phishing, que con mayor frecuencia usan pretextos no bancarios para atraer a usuarios a sitios fraudulentos. Los asuntos de estos envíos ya no suponen ser de su banco, ahora son casos como "Fallece el Potrillo en accidente aéreo", "Derriban avión del Presidente de la República", etc… En Europa es famoso el código llamado **Storm** porque su asunto implicaba "230 muertos por tormenta en Europa". También conocido como **Nuwar**, fue capaz de crear la red de computadoras Zombies (botnets) más grande del mundo.

Gusanos como **Sality** tienen la capacidad de instalarse y abrir puertas traseras en los

2007

equipos (**backdoors**) para enviar a un atacante información sensible recopilada por el Keylogger incluido, tiene capacidad de mutar para no ser detectado, y demuestra capacidad para cerrar software anti-virus en las máquinas atacadas.
En el segundo semestre aparecen códigos que utilizan sistemas de mensajería instantánea como el MSN Messenger para esparcirse.

2008

Dada la enorme popularidad de las redes sociales como Facebook, Hi5, Myspace, Orkut, etc… surgen códigos maliciosos dirigidos a los usuarios de las mismas, con la intención de robar acceso a sus perfiles. Delincuentes recurren a la creación de perfiles falsos con publicidad capaz de atraer a los usuarios más incautos hacia sitios de contaminación.
Toma notoriedad el **Rogue** Malware, código que típicamente se hace pasar por software anti-virus, y bajo la promesa de eliminar amenazas del equipo, termina por contaminarlo más, descargándole código que lo deja vulnerable a ataques remotos.
Aprovechando la masificación del uso de dispositivos USB como memorias y cámaras, se propagan códigos instalados en el archivo **autorun.inf**, que se ejecuta automáticamente y sirve como medio de diseminación para contaminar otros equipos. Esto impacta principalmente a empresas que usan USBs como medio de transmisión de información. Los estudiantes en universidades se ven igualmente afectados pues es el medio preferido para portar documentos escolares.
Las técnicas de Ingeniería Social utilizadas por el Nuwar crecen en eficiencia, y se combinan con otras técnicas residentes en los sitios web a los que consiguen redirigir a usuarios, como el caso del Drive-by-Download, técnica consistente en inyectar código dentro de una página honesta para re-direccionar al visitante a otra idéntica pero maliciosa sin que se percate.
La aparición de gusanos como **Conficker**, que explotan vulnerabilidades del sistema operativo Windows dejan en evidencia la importancia de que todos los usuarios entiendan la importancia de instalar actualizaciones de seguridad en forma automática, o al menos frecuente.

Finalmente, Cuidado con los Virus Falsos!! (Hoaxes)
Debes saber que también circulan en Internet cadenas de virus falsos que solo buscan alarmarte y ocasionalmente inducirte a borrar manualmente archivos de tu equipo, con lo que causan a veces daños similares a los virus reales. Haz click aquí para visitar un sitio que te proporciona mucha información sobre estas cadenas.

No lo olvides!

Instala un Anti-virus y mantenlo actualizado para estar a salvo de todas estas amenazas.