Cronología de los virus informáticos

La historia del malware

Autor: Laboratorio de ESET Latinoamérica
Fecha: martes 14 de Noviembre del 2006
Actualización: jueves 02 de Febrero del 2012

ESET, LLC 610 West Ash Street, Suite 1900
phone: (619) 876 – 5400, fax: (619) 437 – 7045
sales@eset.com, www.eset.com

El ciberespacio. Una alucinación consensual experimentada diariamente por billones de legítimos operadores, en todas las naciones, por niños a quienes se enseña altos conceptos matemáticos…Una representación gráfica de la información abstraída de los bancos de todos los ordenadores del sistema humano. Una complejidad inimaginable. Líneas de luz dispuestas en el no-espacio de la mente, agrupaciones y constelaciones de datos…, el propio terreno de lo virtual, donde todos los medios se juntan (fluyen) y nos rodean.

William Gibson, Neuromante, 1989

El presente documento pretende ser un resumen de los hechos más importantes de los últimos dos siglos, referentes al desarrollo y evolución de los virus informáticos. Si bien no puede considerarse un documento definitivo, por su desarrollo constante, define gran parte de los hitos que marcaron la mencionada evolución.

Génesis: 1800 a 1960

Corría el año 1822. **Charles Babbage** diseña y comienza la construcción de lo que dio a conocer como la máquina diferencial para tabular polinomios.

Mientras tanto en 1883, si bien Bill Gates no soñaba con construir un imperio y Linus Torvalds aún no aprendía a programar, **Thomas Alva Edison** descubre el efecto que lleva su nombre y desde ese momento ya nada volvería a ser lo mismo.

En 1904, el británico **John Ambrose Fleming** utiliza una válvula diodo, denominada diodo Fleming, para pasar corriente alterna a corriente directa. Dos años después, en 1906, el norteamericano **Lee de Forrest** tomando como base el trabajo de Fleming, patenta el tríodo y da nacimiento al primer amplificador electrónico.

Durante 1931, en el MIT (Instituto Tecnológico de Massachussets), **Vannevar Bush** construye un analizador diferencial, o lo que podría llamarse la primera computadora analógica, que servía para realizar automáticamente algunas de las operaciones elementales.

Curiosamente, en el mismo año, el matemático inglés **George Boole** describe el álgebra que lleva su nombre dando origen a lo que en la actualidad se conoce como **ciencia de la computación**.

Pero faltaba unir el mundo mecánico con la información y para eso estaba **Claude Elwood Shannon**, quien en 1937 presenta su tesis de licenciatura en el MIT, estableciendo el paralelismo entre la lógica de Boole y los circuitos de transmisión. Luego, Shanon será recordado como el padre de la "Teoría de la Información".

Por otro lado, también durante el mismo año, el inglés **Alan Mathison Turing** establece las limitaciones de un hipotético ordenador definiendo la llamada "Máquina de Turing", dando origen a la Inteligencia Artificial y a lo que, en 1948, **Norbert Wiener** dio en llamar **Cibernética**.

Si bien existen discrepancias en las fuentes, se sabe que en 1941 el alemán **Konrad Zuse** finaliza su Z3, primera computadora electromecánica digital controlada por un programa completamente funcional. Esta computadora no era de propósito general y supuestamente Zuse diseñó un lenguaje de programación de alto nivel teórico en 1945: el Plankalkül. Luego, en 1950 la Z4 se convertiría en la primera computadora en ser comercializada. Quizás, las discrepancias entre las diferentes fuentes se

deben a que los descubrimientos de Zuse fueron realizados en Alemania durante la segunda guerra mundial.

Llegado el año 1943, el norteamericano **John Presper Eckert** diseña el primer programa mecánico y, junto a su amigo **John Williams Mauchly,** comienza la construcción de la primera computadora decimal de propósito general patentada: ENIAC, finalizada en 1946 en la Universidad de Pensilvania.

Cabe aclarar que muchos autores coinciden en que la primera computadora electrónica digital fue la ABC (Atanasoff-Berry Computer) desarrollada en 1941 por **John Atanasoff** y **Clifford Berry**, y si bien esta nunca fue patentada se sabe que este trabajo pudo influenciar a Mauchly en el diseño de ENIAC.

Mark I, que se suele presentar como la primera computadora, fue diseñada por **Howard H. Aiken** en la Universidad de Harvard cuando corría el año 1944.

Asimismo, en 1946, el húngaro **John Louis Von Neumann**, establece el concepto de programa almacenado (la Arquitectura Von Neumann), con la cual en 1949 se construye EDVAC (Electronic Delay Storage Automatico Computer) en la Universidad de Manchester. EDVAC, a diferencia de su antecesora ENIAC, era binaria y tuvo el privilegio de almacenar un programa.

La arquitectura de Von Neumann señala que las máquinas de calcular deben tener un núcleo compuesto por una unidad de control y su aritmética, y un depósito de memoria.

En 1947 se da el primer gran salto teórico-tecnológico: los premios Nobel **John Bardee**, **Walter Brattain** y **William B. Shockley** diseñan el transistor, con el cual comienza la substitución de los tubos de vacío, disminuyendo considerablemente el volumen de las máquinas.

Muchas fuentes afirman que en 1951, la corporación de Eckert y Mauchly da origen a la primera computadora fabricada comercialmente: UNIVAC I, la primera en utilizar un compilador para que la máquina pudiera interpretar un programa. Como se puede apreciar, esta información es contradictoria con respecto a la afirmación sobre que la primera computadora comercializada fue la ya mencionada Z4.

En 1954, se construye la IBM 650, considerada la primera computadora de producción masiva habiendo 100 de ellas en todo el mundo; Y durante 1957, nace el primer lenguaje de programación de alto nivel desarrollado por la empresa IBM (International Business Machine) llamado FORTRAN.

El luego premio Nobel **Jack S. Kilby**, empleado de la compañía informática estadounidense Texas Instruments, desarrolla en el año 1959 el microchip.

En 1960 el DEC PDP-1, precursor de las minicomputadoras y fabricada por DEC (Digital Equipment Corporation) introduce el cinescopio, considerado el primer monitor de computadora. Debido a que esta

computadora sólo necesitaba un operador para atenderla, inspiró a los primeros "hackers" en el MIT a programar en esta máquina, el primer juego de vídeo de computadora: el SpaceWars.

En 1964, IBM anuncia el lanzamiento del Sistema/360, la primera familia de computadoras compatibles, lo que lleva a que **John Kemeny** y **Thomas Kurtz** desarrollaran, en el Darmouth Collage, el BASIC (Beginners All-purpose Symbolic Instruction Code), siendo el origen de los lenguajes de programación modernos.

La primera PC (Personal Computer, en español, Computadora Personal) nace en 1971. La **Kenbak 1**, fue fabricada por **John Blankenbaker** de la Kenbak Corporation de Los Angeles. Esta computadora estaba dirigida al mercado educacional y contaba con 256 bytes de memoria RAM. Se comercializaron 40 equipos al costo de U$S 750.

Dos años después, aparece la primera computadora personal comercial, la Altair 8800, diseñada por **Ed Roberts** y **Bill Yates**, fabricada por la empresa MITS y vendida a U$S 350. Sin embargo, la primera PC en lograr uso masivo fue la Apple I presentada en 1976. En 1977 las empresas Apple, Commodore y Tandy distribuyen los primeros ordenadores completamente ensamblados.

En agosto de 1981, IBM entra en escena estableciendo un estándar con la primera PC de propósito general distribuida con el sistema operativo PC-DOS (posteriormente MS-DOS). En este punto, se puede decir que la historia le juega una mala pasada a **Gary Kildall**, desarrollador del sistema operativo CP/M en 1975 (capaz de ejecutarse en la Altair 8800) y a quien IBM no pudo contactar por diversos motivos.

Así, IBM termina adoptando MS-DOS, copia casi fiel de QDOS (Quick and Dirty OS) de **Tim Paterson,** a su vez clon de CP/M, el cual **William Henry Gates III (Bill Gates)** compra y realiza pequeñas modificaciones antes de llegar a un acuerdo de explotación con IBM.

Pero… ¿qué tiene que ver todo esto con el tema central? Simplemente que el origen de los virus informáticos se encuentra allí; en el mismo lugar que el origen de la computación moderna, en el álgebra de Boole, en la teoría de la información de Shannon, en la máquina de Turing, en la cibernética de Wiener, en la Inteligencia Artificial y en los modelos matemáticos de Von Neumann.

El origen y el futuro de los virus informáticos están allí: en los inventos que revolucionaron el siglo pasado, los cuales intrigan a los investigadores de este milenio y en lo que se perfila como el origen de las "máquinas pensantes al servicio del hombre".

Prehistoria: 1948 - 1983

En 1948 Von Neumann ya daba conferencias hablando de autorreproducción de las máquinas. Sólo el sentido común le decía que una máquina sería capaz de reproducirse, al igual que lo hace un animal, si la misma contaba con las "moléculas" necesarias.

Von Neumann ya había establecido la idea de programa almacenado y en 1949 avanza en sus investigaciones escribiendo un artículo exponiendo la Teoría y organización de autómatas complejos (Theory and Organization of Complicated Automata). En este documento, se presentaba por primera vez la posibilidad de desarrollar pequeños programas replicantes y capaces de tomar el control de otros programas de similar estructura.

El texto de este artículo ha sido incluido en el libro "Theory of Self-Reproducing Automata" completado, editado y publicado en forma póstuma en 1966 por **Arthur Burks**.

Sus inquietudes por la capacidad de las máquinas de autoreplicarse, lo lleva a sentar los precedentes de lo que hoy denominamos "máquinas de Von Neumann" o "autómatas celulares", máquinas capaces de reproducirse a sí mismas en pro de un objetivo común: la auto-reproducción. En 1951, Neumann propuso diferentes métodos mediante los cuales demostró como crear autómatas celulares.

Sin bien el concepto tiene miles de aplicaciones en la ciencia, modelando y simulando gran cantidad de sistemas físicos, como fluidos, flujo de tráfico, etc.; es fácil apreciar una aplicación negativa de la máquina de Von Neumann: los virus informáticos, programas que se reproducen a sí mismos el mayor número posible de veces, aumentando su población de forma exponencial.

En 1959, el matemático Británico **Lionel S. Penrose** presentó su punto de vista sobre la reproducción automatizada en un artículo llamado "Self-Reproducing Machines" publicado en la revista *Scientific American*. Penrose describe programas capaces de activarse, reproducirse, mutar y atacar haciendo la analogía con estudios propios anteriores en donde ciertas estructuras podían replicarse desde una "semilla". Luego de un tiempo, **Frederick G. Stahl** reproduce este modelo en un programa capaz de "vivir" para la IBM 650.

En el mismo año, en los laboratorios de la Bell Computer, tres jóvenes programadores**: Robert Thomas Morris** (no confundir con su hijo Robert Tappan Morris de quien se hablará luego), **Douglas McIlroy** y **Victor Vysottsky** crean un juego denominado **CoreWar**, inspirados en la teoría de Von Neumann.

CoreWar (el precursor de los virus informáticos) es un juego en donde programas combaten entre sí con el objetivo de ocupar toda la memoria de la máquina eliminando así a los oponentes. La primera "guerra"

desarrollada fue "Darwin" y estaba programada en RedCode (no confundir con el gusano del que se hablará posteriormente), una especie de pseudo-lenguaje assembler limitado.

CoreWar fue mantenido en el anonimato, como entretenimiento para intelectuales durante muchos años y recién en 1984, **Ken Thompson** (creador del sistema operativo Unix y el lenguaje de programación B) lo saca a la luz al momento de recibir el premio Turing de A.C.M. (Asociation of Computing Machinery), e insta a la comunidad a experimentar con estas "criaturas". Además se forma la International Core War Society (ICWS) y se actualizan las reglas del juego con las que actualmente se sigue jugando en Internet.

En 1970, el Dr. **Gregory Benford** (físico y escritor de ciencia ficción) publica la idea de un virus en el número del mes de mayo de Venture Magazine, describiendo específicamente el término **computer virus** y dando un ejemplo de un programa denominado **vacuna** para eliminarlo.

El que se considera el primer virus propiamente dicho y que fue capaz de "infectar" máquinas IBM 360 a través de una red ARPANET (el precedente de la Internet actual), fue el llamado **Creeper**, creado en 1972 por Robert Thomas Morris. Este parásito emitía un mensaje en la pantalla periódicamente: "I´m a creeper… catch me if you can!" (Soy una enredadera, atrápame si puedes).

Para eliminar a Creeper se creó un programa llamado **Reaper** (segadora) programado para buscarlo y eliminarlo. Este es el origen de los actuales **antivirus**.

En 1974 aparece **Rabbit** (conejo), llamado así porque no hacía nada excepto reproducirse.

En enero de 1975, **John Walker** (fundador de Autodesk) descubre una nueva forma de distribuir un juego en su UNIVAC 1108 e inadvertidamente da origen al primer troyano de la historia. El mismo recibe el nombre **"Animal/Pervade"**; Animal debido a que el software debía adivinar el nombre de un animal en base a preguntas realizadas al usuario, y Pervade que era la rutina capaz de actualizar las copias de Animal en los directorios de los usuarios, cada vez que el mismo era ejecutado, de allí que sea un troyano.

Debido a esta forma de auto-actualización, el programa tenía la capacidad de "aprender" de sus errores sobrescribiéndose a sí mismo cada vez que se "equivocaba". Sin embargo, un error en la programación del juego hacía que existieran múltiples copias de sí mismo en diversos directorios de la máquina. La solución a este problema de programación fue crear una versión del juego que buscara versiones anteriores y las eliminara.

A finales de los setenta, **John Shoch** y **Jon Hupp**, investigadores del Centro de Investigación Xerox de Palo Alto, California, intentaron darle un uso práctico a los CoreWars, creando un programa que se encargara de las tareas de mantenimiento y gestión nocturnas, propagándose por todos los sistemas del centro. Lamentablemente, este "trabajador virtual" bautizado como **worm** (haciendo mención a la novela The Shockwave Rider, escrita en 1975 por John Brunner) se extendió por toda la red y causó grandes problemas, por lo que se decidió la eliminación completa del mismo.

Este experimento fallido quizás haya sido la primera aproximación de procesamiento en paralelo logrado por un programa auto-replicante, tan común hoy en día.

Ya en la década de los ochenta, las computadoras ganaban popularidad gracias a su rápida evolución y cada vez más personas entendían informática y escribían sus propios programas. Esto también dio origen a los primeros desarrolladores de programas dañinos.

En 1981, **Richard Skrenta** (co-fundador de NewHoo, actual DMOZ, el servicio de directorio Internet en el cual está basado Google) recibe una Apple II como regalo y escribe el primer virus de amplia reproducción: **Elk Cloner** el cual se almacenaba en el sector de inicio de los disquetes de 360 kb de capacidad y era capaz de residir en memoria luego que el disco era retirado. Elk Cloner era inocuo para el sistema, pero contaba la cantidad de arranques y cuando llegaba a cincuenta mostraba el siguiente poema:

Elk Cloner: The program with a personality (Elk Cloner: El programa con personalidad)
It will get on all your disks (llegará a todos tus discos)
It will infiltrate your chips (se infiltrará en sus chips)
Yes it's Cloner! (sí, es Cloner!)
It will stick to you like glue (se te pegará como el pegamento)
It will modify ram too (modificará la ram también)
Send in the Cloner! (envía el Cloner!)

La velocidad de desarrollo, de avance de la tecnología y la necesidad de "ser el primero" ya se hacía presente en esa época, ya que debido a esta urgencia de mercado el sistema operativo provisto por IBM (el MS-DOS) adolecía de grandes agujeros que permitieron la aparición de códigos maliciosos y su rápida expansión.

Definiciones: 1983 - 1989

El artículo "Experiments with Computer viruses" de **Frederick B. Cohen** publicado en 1984 (y republicado en 1987 en "Computers and Security", Vol. 6, pág. 22-35), cuenta que el primer virus informático fue desarrollado para una demostración de **Leonard Adleman** (la "A" del cofundador de RSA y del popular algoritmo del mismo nombre) en un seminario de seguridad informática.

Luego de una semana de trabajo sobre un sistema Unix en un VAX 11/750, el 10 de noviembre el primer virus es introducido sobre el comando **vd** de Unix, luego de la obtención de los permisos necesarios.

Después de esta primera presentación, nuevos experimentos fueron planteados para los sistemas más importantes de ese momento, pero los permisos fueron rechazados por las posibles consecuencias que ya se habían podido entrever.

Sin embargo, luego de esta primera experiencia, se realizaron otras sobre distintos sistemas, con el fin de demostrar las posibles consecuencias de estos programas y las posibles formas de solución. Por ejemplo, en 1984 se desarrollaron pruebas en un sistema Bell-Lapadula (basado en roles, usuarios y permisos). El virus que se ejecutaba sobre un Univac 1108 (realizando tareas legítimas del sistema sin utilizar bugs o vulnerabilidades del sistema) demostró su capacidad de moverse de un nivel de seguridad a otro realizando escalada de privilegios.

Los experimentos con virus han "dado sus frutos", pero no se puede decir lo mismo de las soluciones, ya que las mismas aún no habían sido estudiadas ni desarrolladas.

En 1983, el aún estudiante Cohen inicia su estudio sobre los virus y en 1985, finaliza su tesis de doctorado, basada en "programas auto-duplicadores". El tutor de esta tesis fue el Dr. Adleman, y quizás de allí provengan las confusiones sobre quien ha sido el primero en acuñar el término virus y sus definiciones posteriores.

En 1984, Cohen publica sus estudios en "Computer Viruses - Theory and Experiments", donde define por primera vez a los **virus**, palabra que ya había sido ampliamente difundida luego de los trabajo de Adleman. La definición propuesta por Cohen y aceptada por la comunidad fue:

"Programa que puede infectar a otros programas incluyendo una copia posiblemente evolucionada de sí mismo"

Debido a esta definición y a su tratamiento formal, Cohen es conocido como el "padre de los virus", aunque, como ya se mencionó, no fue el primero en trabajar sobre ellos.

Este documento también sienta los precedentes de programas para combatir a estas amenazas y demuestra que "no hay ningún algoritmo general que pueda concluir con total fiabilidad (100%) si un programa es o no un virus". Para ello se valía de la siguiente demostración por reducción al absurdo:

"Supóngase que existe un algoritmo general "A" que, analizando cualquier programa "P", devuelve "true" si y sólo si "P" es un virus. Entonces sería posible crear un programa "P", que hiciera lo siguiente:

```
si ( A(P) = falso ) entonces
        infectar el sistema
si ( A(P) = verdadero ) entonces
        no infectar
```

Es decir: "P" es un virus si "A" dice que no lo es; y no lo es si "A" dice que lo es. Por contradicción, ese algoritmo general "A" no existe."

Además, Cohen menciona las posibles formas de detección de un virus y las clasifica en:

- Detección por apariencia
- Detección por comportamiento
- Detección por evolución de otros virus conocidos
- Detección por mecanismos de engaño

Cohen no se equivocaba, ya que todas esas técnicas son utilizadas actualmente por los antivirus modernos. Tampoco se equivocaba al extraer como conclusión que para estar seguros contra un ataque viral, el sistema debe proteger el flujo de información que ingresa y que sale del mismo.

En 1987, **Tom Duff** comienza a experimentar en sistemas Unix con pequeños *scripts* probando que los virus no necesariamente debían infectar archivos dependientes del sistema y arquitectura para el cual fueron creados.

Luego, en 1989 Duff publica un artículo llamado "Experience with Viruses on Unix Systems" describiendo (y mostrando) un virus que infectaba archivos ejecutables, de diferentes sistemas Unix, sin modificar el tamaño del mismo. El virus (de 331 bytes) se copiaba en ejecutables que tuvieran un espacio de 331 bytes (o mayor) ocupado con ceros y modificaba el punto de entrada del binario para que apuntara al virus. Este concepto fue ampliamente explotado por los virus de la siguiente generación.

Luego de las controversias desatadas por su artículo, Duff desarrolló lo que podría denominarse antivirus, el cual restauraba el punto de entrada de ejecución al archivo verdadero. Cada programa reparado quedaba "vacunado" y no podía ser re-infectado por el virus, a menos que se creara una variante del mismo. Este concepto de "vacuna inmunizadora" también fue aprovechado por la nueva generación de antivirus.

Duff, al igual que Cohen, había llegado a la conclusión que "no hay manera de hacer un sistema que sea inmune y útil al mismo tiempo".

En 1988, Adleman en su artículo "An Abstract Theory of Computer Viruses" introduce el concepto de **Cuarentena** y lo define como "un sistema aislado para la ejecución de programas antes de introducirlos en un ambiente donde hagan daño".

Además, incluye los términos **desinfección,** definiéndolo como "un procedimiento capaz de volver un programa infectado a su estadio anterior a la infección"; y **certificación**, para aquello "que asegure que un programa determinado no está infectado".

En el mismo documento también se define formalmente el término **troyano** como "programa alojado dentro de otra aplicación u otro elemento de apariencia inocente, que se instala en el sistema al ejecutar el archivo que lo contiene".

Evolución: 20 años y contando

1986

En este año se detecta la primera epidemia de un virus totalmente compatible con los IBM PC. Este virus, llamado **Brain**, fue desarrollado por el programador pakistaní Basit Farrq Alvi y sus hermanos Shahid y Amjad, era capaz de infectar la zona de arranque, cambiar el nombre del disco a "(c) Brain" y fue el primero en utilizar técnicas tipo Stealth (esconder modificaciones realizadas a los archivos o al sector de arranque) para ocultar su presencia.

Brain incluía una línea de texto que contenía los nombres de los programadores, direcciones y número de teléfono. Esta información era suministrada ya que según los hermanos este programa sólo era un experimento antipiratería (que los hizo famosos a ellos y a su empresa Brain Computer Services) y nunca tuvieron la intención de hacer daño. Quizás esto se confirme al ver que el virus no contenía carga dañina en su código.

*Welcome to the Dungeon (c) 1986 Basit * Amjad (pvt) Ltd. BRAIN COMPUTER SERVICES 730 NIZAM BLOCK ALLAMA IQBAL TOWN LAHORE-PAKISTAN PHONE: 430791,443248,280530. Beware of this VIRUS.... Contact us for vaccination...*

Los hermanos se dieron cuenta de la epidemia desatada cuando comenzaron a recibir llamadas de distintos lugares del mundo exigiendo la limpieza de sus sistemas. El primer espécimen *"in-the-wild"* fue encontrado en la Universidad de Delaware (EE.UU.).

Basado en la tesis de Cohen, en 1986 un ingeniero llamado **Ralf Burger**, crea un virus operativo, al que llamó **Virdem** (demostración de virus). **Virdem** infectaba archivos ejecutables con extensión .COM y estaba programado para auto-reproducirse y borrar archivos del sistema huésped. Se trató del primer virus que utilizó la siguiente característica: reproducirse y causar daño. Este virus pasó a la historia, porque

Burger lo repartió en diciembre de ese año en una convención organizada por el Chaos Computer Club en Hamburgo, Alemania.

En esta convención se trata por primera vez el tema social de los virus expresando "que su creación se debía principalmente a la mala posición social de los programadores" y que "el problema no eran los virus, sino la dependencia de la tecnología".

1987

En 1987, Burger escribe un libro que trata sobre los virus informáticos: "Computer viruses: A high-tech disease", similar a otro de **B. Khizhnyak** llamado "Writing virus and antivirus".

Aunque Burger "olvida" mencionar los virus de arranque, como Brain, incluye el código fuente del virus **Vienna** y de su solución, provocando el primer gran escándalo alrededor de este tema.

Vienna era un virus extremadamente sencillo, no residente en memoria, capaz de infectar sólo archivos .COM sobre el sistema operativo MS-DOS 2.0, o superior, y de modificar los segundos de la hora del sistema al valor "62".

La publicación de Burger da origen a lo que hoy en día recibe el nombre de **variantes**, ya que muchos programadores experimentaron la creación de "su propio virus" a partir del publicado por Burger. La "familia" del virus Vienna, es innumerable y se propagó por todo el mundo.

La historia de Vienna ha estado cubierta de un manto de intrigas desde su aparición, ya que nunca se ha confirmado la identidad de su creador. Actualmente existen dos versiones al respecto.

La primera indica que **Franz Swoboda** fue la primera persona que detectó el virus y lo llamó Charlie. Mucha información apuntaba a Ralf Burger como autor, pero este rechazó siempre la historia e incluso declaró haber recibido el virus de Swoboda.

La segunda versión señala que Vienna en realidad fue creado en Austria (de allí su nombre) como experimento por un estudiante. Quizás lo más plausible en este sentido es que el virus realmente se haya creado en Viena y llegado a Swoboda de alguna forma.

Más allá de este desacuerdo, Ralf Burger envía una copia al investigador **Bernt Fix**, quien lo desensambla y crea un programa para neutralizarlo. Es decir que Fix (curioso nombre en inglés en este contexto) fue el precursor de los antivirus actuales. En consecuencia, Burger publica en su libro el código utilizado para neutralizar a Vienna, tomando como base el trabajo de Fix.

En 1987, también aparece **Lehigh** (aparentemente experimentos de Cohen y **Ken van Wyk**) en la universidad que le dio nombre, siendo uno de los primeros virus dañinos. Para ese entonces, los expertos en virus ya conocían las formas de actuar, por eso el virus nunca dejó la universidad y Lehigh nunca fue detectado en el exterior.

Otro evento notable en este año fue la aparición del primer virus capaz de infectar computadoras Macintosh: **MacMag**. Un empleado de Aldus Corporation se infecta con un disco de juegos y luego el virus es distribuido al público en copias de su software Aldus Frenhand 10.

MacMag, también conocido como Brandow, Drew y MacPeace, fue escrito y diseminado a finales de 1987 y principios de 1988. Sus desarrolladores fueron los editores de la revista de computación canadiense "MacMag" **Artemus Barnoz** (alias Richard Brandow) de 24 años y **Boris Wanowitch** (de allí los múltiples nombres de este virus).

Barnoz distribuyó copias del virus a través de los disquetes que entregaba a los miembros del club Mac del cual era presidente. Otras características que hacen único a MacMag es que logró su propagación meses antes de la aparición del "gusano de Morris", se propagaba en disquetes y por lo tanto era un verdadero virus, no un gusano.

Además, MacMag también se propagó a través de Compuserve y por los Bulletin Board Systems (BBS), servicios en línea anteriores a Internet.

Este virus se limitaba a presentar un mensaje de paz en pantalla y al llegar el día 2 de Marzo de 1988 (fecha del aniversario de la aparición del Macintosh II) se autoeliminaba.

A finales de 1987 hace su aparición el virus **Jerusalem** o **Viernes 13** (modificaciones de su antecesor **suriV**) y capaz de infectar archivos con extensión .EXE y .COM. Su primera aparición fue reportada en la Universidad Hebrea de Jerusalem y llegó a ser uno de los más famosos de la historia.

En Alemania, el investigador **Wolfang Stiller** reporta la aparición del complejo **Cascade**, también conocido como **Falling Letters** y primer virus encriptado en conocerse, capaz de infectar archivos .COM.

En la navidad del mismo año, IBM se vio colapsada por lo que técnicamente era un gusano de correo electrónico semejante a las tarjetas virtuales actuales. El 25 de diciembre, el gusano mostraba un árbol de navidad en sistemas VM/CMS junto al mensaje "*run this script*", mientras se enviaba a la lista de direcciones del usuario infectado. Al recibir el correo, las personas ejecutaban el script y la infección continuaba. Debido al volumen de mensajes enviados, se produjo una denegación de servicio en los servidores de IBM.

Si bien los autores del gusano nunca se conocieron, este hecho junto a la infección de IBM con el virus Cascade, hicieron que la compañía comience a considerar la problemática de los virus de manera seria..

1988

Aparece **Stoned**, también conocido como **Marijuana** debido a su popular mensaje *"LEGALISE MARIJUANA"*. Se cree que su origen es Nueva Zelanda ya que desde allí se reportaron los primeros casos.

En marzo, es encontrado en la Universidad de Turín el virus **Ping Pong** haciendo honor al juego de la pelotita (el ♦) que rebotaba en pantalla e infectaba la zona de arranque del disco. Versiones posteriores de este virus eliminaron el efecto visual y perfeccionaron las formas de infección.

El 2 de noviembre de 1988, **Robert Tappan Morris** (hijo de Robert Thomas), estudiante de 23 años del MIT (Instituto Tecnológico de Massachusetts), crea el primer gusano de reproducción masiva, infectando y colapsando el 10% de ARPANET, la Internet de ese entonces, incluyendo la NASA y el MIT, durante 72 horas. Este programa pasaría a la historia como el **Gusano de Morris**.

Para reproducirse este gusano aprovechaba una vulnerabilidad en los sistemas operativos UNIX presente en las plataformas VAX y Sun Microsystems, además de recolectar contraseñas de los sistemas afectados. Si se lo extrapola a la actualidad se podría decir que el gusano de Morris fue el primer programa capaz de aprovechar agujeros en los sistemas (sendmail de Unix en este caso) para lograr sus propósitos.

Finalmente, el 22 de enero de 1990, Morris hijo fue enjuiciado por fraude y engaño y condenado en la Corte Federal de Syracuse, Nueva York. Sin embargo, el juez expresó que "no creía que los requisitos (fraude y engaño) de la sentencia se dieran en el caso del acusado", y por lo tanto lo sentenció a tres años de libertad condicional, una multa de U$S 10.000 y 400 horas de servicio comunitario.

Esta, por algunos llamada catástrofe, quizá fue el disparador para que por primera vez la comunidad informática y científica, diera crédito a las posibles consecuencias de un ataque masivo a una red mediante programas auto-replicantes.

Como dato anecdótico, el 20 de septiembre, en Texas, el programador **Donald Gene Burleson** es sometido a juicio por contaminar intencionadamente un sistema. Es la primera persona juzgada con la ley de sabotaje que entro en vigor el 1 de septiembre de 1985. Gene fue declarado civilmente culpable y condenado a siete años de libertad condicional y a pagar la suma de U$S 12.000.

A finales de este año, el virus Jerusalem se había expandido por diferentes países y esto llevo a que algunas compañías comenzaran a ver el tema de los virus con especial interés, si bien algunos notables profesionales insistían en que estas amenazas seguían siendo el "producto de mentes proclives a la ciencia ficción".

Debido a la expansión que habían logrado algunos virus, el programador del Reino Unido Dr. **Alan Solomon** comenzó a desensamblarlos y a crear sus propias herramientas de detección y desinfección para que "la gente pudiera controlar a los virus". Es así que en este año, el antivirus Dr. Solomon´s Anti-

Virus Toolkit es lanzado al mercado y ampliamente utilizado hasta que fuera adquirido por la empresa Network Associates Inc. (NAI) creadora del popular programa Scan.

1989

En Bulgaria nace el virus **512** que infectaba archivos .COM y tenía capacidades stealth. Su descubridor fue el Dr. **Vesselin Vladimirov Bontchev**, un importante investigador de virus del mismo país.

De hecho, este fue el año de lanzamiento de la denominada "fábrica búlgara de virus" con el escritor **Dark Avenger** (o Eddie) a la cabeza, quien es reconocido como uno de los más prolíficos creadores de virus con técnicas originales. Su principal creación es el virus que lleva su nombre y que fue el primero en explotar de manera conjunta técnicas stealths y polimórficas infectando archivos .COM y .EXE.

Es importante remarcar que Dark Avenger y Vesselin V. Bontchev no son la misma persona, si bien existe una leyenda urbana que puede llevar a esa confusión.

De esta fábrica es importante recordar los virus: Dir, Dir II, Int13, Murphy, Nomenclatura, Darth Vader y Vacsina; todos ellos con técnicas de infección exclusivas y no explotadas hasta ese momento.

También aparece el peligroso **Datacrime** que formateaba a bajo nivel el cilindro cero (donde se aloja la FAT) del disco y que sólo actuaba desde el 13 de octubre hasta el 31 de diciembre. Este virus originó la venta del programa anti-datacrime a U$S 1, que si bien tenía numerosos fallos sirvió de base para las herramientas antivirus comerciales de los próximos años.

En octubre de 1989, Cascade hizo que el Dr. **Eugene Kaspersky**, de origen ruso, se interesara en la investigación de este tipo de programas. Kaspersky es el desarrollador de AVP Antiviral Toolkit Pro de la desaparecida compañía S&S International y es co-fundador de Kaspersky Lab en 1997. AVP fue renombrado a Kaspersky Anti-Virus en noviembre del año 2000.

En 1989 aparece otro grupo de compañías antivirus, entre las que se destacan:

- **F-Prot**, creado por **Fridrik Skulason** en una compañía de origen islandés llamada Frisk Software International.
- **ThunderByte** de la empresa holandesa ESaSS, considerado como uno de los más rápidos y mejores antivirus de la época, especialmente por su motor heurístico. Fue el primero en explotar la importancia de la heurística en la detección de virus y de permitir el agregado de firmas creadas por el usuario. Posteriormente, en 1995 este antivirus fue adquirido por la compañía Norman Virus Control.
- **IBM Virscan**, un producto originalmente de uso interno del gigante azul y que decidió comercializar por presión pública. Salió a la venta en Octubre de 1989.

Otro hecho destacable durante este año es la distribución por correo electrónico de 20.000 copias del "*Aids Information Diskette*", a usuarios que figuraban en bases de datos de diversos organismos. El paquete contenía un disquete con un programa (con supuesta información del SIDA) que evaluaba ciertas condiciones y cuando se daban las mismas, procedía a cifrar el disco rígido presentando una "factura" a la víctima para recuperar la clave de cifrado. Este fue el origen de los actuales **Ransomware**.

1990

Haciendo gala de la inventiva búlgara, aparece la primera VX-BBS de intercambio de virus, permitiendo descargar cualquier virus siempre y cuando se haya dejado alguno previamente. Esto también marca la importancia y la diferencia entre el desarrollo y la propagación de virus.

La revista inglesa PC Today distribuye, por error, el virus **DiskKiller** en una de sus publicaciones y el mismo se trasforma en epidemia. En la segunda mitad del año aparecen **Frodo** y **Whale**, que usaban un complejo algoritmo para camuflarse en el sistema.

Mark Washburn, basándose en el libro de Burger y en el virus Vienna, crea **Chameleon**, el cual era capaz de mutar con cada infección (polimórfico). Esta característica hizo que algunos antivirus basados en detección por firmas resultaran inútiles y los obligara a replantear sus tecnologías, por ejemplo hacia la heurística.

Al 18 de diciembre de 1990 la lista de productos antivirus era la siguiente:

- AntiVirus Plus de Iris
- Artemis, posteriormente conocido como Panda
- Certus de Certus International
- Data Physician de Digital Dispatch
- Dr. Solomon´s Anti-Virus Toolkit de S&S
- F-Prot de Frisk Software
- ThunderByte de ESaSS
- Turbo Antivirus de Carmel
- Virex-PC de Microcom
- Vaccine de Sophos
- Vaccine de World Wide Data
- V-Analyst de BRM
- Vet de Cybec
- Virscan de IBM
- VirusBuster de Hunix
- Virucide (McAfee´s Pro-Scan) de Parsons

- Virusafe de Elia Shim
- ViruScan de McAfee
- Vi-Spy de RG Software

En diciembre de ese año se funda una organización sin fines de lucro llamada **EICAR (***European Institute for Computer Antivirus Research***)** en Hamburgo, Alemania, y se crea un archivo que lleva el mismo nombre con la finalidad de probar la eficacia de los programas antivirus sin involucrar el riesgo de trabajar con un virus real. El archivo contiene el siguiente código:

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

1991

Se hace evidente que con la cantidad de antivirus existentes, las técnicas para nombrar a los virus son demasiadas confusas por lo que se crea **CARO** *(Computer Antivirus Research Organization***)** para solucionar este problema. Originalmente la organización estaba formada por Fridrik Skulason, Editor de Virus Bulletin y autor de F-Prot; Alan Solomon, de S&S International y Vesselin Bontchev, Universidad de Hamburgo.

CARO decide que los virus deben bautizarse de la siguiente manera (según "A New Virus Naming Convention"):

Family_Name.Group_Name.Major_Variant.Minor_Variant[Modifier]

Si bien esta nomenclatura se sigue respetando (Prefijo.Nombre.Variante), aún hoy en día la problemática del nombre que reciben los virus sigue vigente. Además, nacen Norton Antivirus y Central Point Antivirus.

1992

El 6 de marzo, la aparición de **Michelangelo** (virus de arranque y variante de Stoned) hace que este año sea un hito en la historia, ya que los virus informáticos son masivamente expuestos a la opinión pública.

Michelangelo fue aislado por primera vez en 1991 en Nueva Zelanda y si bien no era un virus peligroso, sus efectos fueron magnificados por la prensa disparando la venta de programas antivirus.

Al parecer su autor era admirador del artista italiano ya que en su código puede leerse:

MICHELANGELO di Ludovico Buonaroti Simoni, born March 6, 1475

Caprese, Republic of Florence…

Por su parte, las capacidades de Dark Avenger seguían creciendo y este virus dio origen a varios motores automáticos de creación de virus. El primero de éstos fue el **MtE** (*Self **Mut**ating **E**ngine*) creado por el mismo Dark Avenger y con manual de uso incluido. Otros constructores dignos de ser mencionados son VCL y PS-MPC.

También aparece **Peach**, primer virus capaz de "atacar" la base de datos de un antivirus y **EXEBug** capaz de controlar la CMOS para prevenir el booteo desde disquetes limpios. También se descubre **Win.Vir_1_4**, el primer virus capaz de infectar ejecutables de Microsoft Windows 3.x. En su código podía leerse lo siguiente:

Virus_for_Windows v1.4
MK92
AntiWindoze Virus by Xavirus Hacker. THNX2MK!!!

En Eslovaquia se funda la compañía de seguridad antivirus ESET, con oficinas centrales en Bratislava, capital del país, y en San Diego, EE.UU. Como los primeros virus atacaban los sectores de arranque de los discos rígidos (ubicados al borde del mismo), se tomó el concepto de "hospital" para describir de manera análoga a un antivirus basándose en un popular programa de TV que se transmitía en aquella epoca por la televisión checoslovaca llamado "*Nemocnica na Okraji Mesta*" ("Hospital al Borde de la Ciudad").

En consecuencia, se decidió nombrar al recientemente creado programa antivirus como: "**N**emocnica na **O**kraji **D**isku" (NOD). Cuando los procesadores de 32-bits aparecieron, se creó un nuevo programa desarrollado desde cero para funcionar sobre esta nueva plataforma. Así fue como nació "**N**emocnica na **O**kraji **D**isku 32" (NOD32).

1993

Durante años el experto antivirus **Joe Wells** había recolectado información sobre la evolución de los virus en el mundo real y, en julio de 1993, crea una lista con 104 virus denominada **WildList**. Actualmente esta lista cuenta con la participación de 80 investigadores de todo el mundo.

Microsoft lanza su propio antivirus: Microsoft AntiVirus (MSAV), basado en Central Point AntiVirus (CPAV). Si bien este antivirus no volvió a aparecer en las versiones sucesivas de los sistemas operativos de Microsoft, no sería este el último intento de la empresa por entrar en este competitivo mundo.

Además, la compañía IBM lanza su propio antivirus para PC-DOS 6.1.

En septiembre ocurrió un hecho que muchos clasificaron como irresponsable: **Mark Allen Ludwig** publica "Computer Viruses, Artificial Life and Evolution". A este libro seguirán dos más en 1995 y 1996 bautizados como el "Pequeño Libro Negro de los Virus Informáticos".

El tratamiento de los virus desde el punto de vista filosófico de su origen, existencia y evolución es sobresaliente. Más allá de eso, la controversia radica en la publicación de código fuente de virus funcionales y sobre la filosofía de la libre publicación proclamada por Ludwig en sus libros y revistas.

1994

Entre los eventos más destacables de este año se encuentra la sentencia a 18 meses de prisión de **Christopher Pile** (alias Black Baron) por parte de Scotland Yard en Inglaterra. Pile fue acusado de ser el autor de los virus **Pathogen**, **Queeg** y del generador **SMEG**. Es la primera vez que un escritor de virus es acusado legalmente y sentenciado.

1995

Con el nacimiento de Microsoft Windows 95 aparecen nuevos conceptos de infección y para confirmarlo, **Sarah Gordon** descubre **Concept** infectando miles de documentos de Microsoft Word, un ámbito hasta el momento inexplorado. Concept fue el primer virus de macro escrito en lenguaje WordBasic de Microsoft y capaz de infectar cualquier plataforma sobre la que se ejecutara MSWord (PC y Mac).

La proliferación de este virus fue tal que llegó a ser el más común en el mundo durante un largo período de tiempo detectándose cientos de variantes.

Microsoft envía versiones infectadas con el virus **From** a sus beta-testers, DEC distribuye accidentalmente copias de Concept en una conferencia en Dublín y la editorial Ziff-Davis distribuye virus en dos de sus publicaciones.

A finales de este año, nace el mítico grupo español **29A**, formado por amigos "con intereses y conocimientos en el campo vírico que llevaban meses intercambiando información, inventando nuevas técnicas, etc.". Su líder, **Mister Sandman**, recopiló el material en una e-zine (**e**lectronic maga**zine**): "tras largas horas de trabajo y arduas conversaciones, en diciembre de 1996, distribuimos nuestro primer número".

Vale la pena remarcar que 29A era un grupo de programadores dedicados a la investigación y desarrollo de vida artificial, en palabras de sus creadores: "*we create life*" ("nosotros creamos vida"). Su laboratorio dio origen a variadas técnicas de infección e innovadores virus informáticos los cuales no contienen rutinas de daño o destrucción.

1996

Si bien el desarrollo de virus se había estancado, en febrero de este año es detectado en Australia **Boza** (o **Bizatch** según sus creadores: el grupo **VLAD**), el primer virus capaz de infectar archivos de 32-bits de Microsoft Windows NT, y del recién estrenado Microsoft Windows 95. Este primer paso alienta a otros grupos como IKX y 29A al desarrollo de virus.

Durante este mismo año, es hallado un complejo virus creado para sistemas Microsoft Windows 95 llamado **Zhengxi**, escrito por el ruso **Denis Petrovym**. Zhengxi era un virus polimórfico, residente en memoria, infector de archivos EXE, LIB y OBJ, stealth y capaz de insertar droppers (archivo ejecutable que contiene otros archivos en su interior) en formato COM en los ficheros ZIP, ARJ, RAR, HA y en EXE self-extracting.

En junio aparece el virus **AEP,** el primer virus capaz de infectar archivos ejecutables de OS/2, un sistema operativo de IBM. En julio, se descubre en Alaska y África, **Laroux**, el primer virus capaz de infectar macros en archivos de Microsoft Excel.

La aparición de los macro virus ya no se detendría por varios años y esta tendencia fue impulsada por la aparición de dos constructores de macrovirus: **Word Macro Virus Construction Kit** (de **Nightmare Joker**) y **Macro Virus Development Kit** (de **Wild Worker**).

En este mismo año Microsoft continúa teniendo problemas. En esta ocasión varios de sus documentos se vieron afectados por el macro virus **Wazzu**.

1997

En febrero aparecen **Staog** (escrito en Assembler por el grupo **Quantum/VLAD**) y **Bliss**, los primeros virus para archivos ELF del emergente sistema operativo Linux. Este último, incluso puede ser compilado para SunOS, Solaris y OpenBSD sin problemas.

Si los virus para Linux no habían causado el revuelo necesario, en este año aparece **ShareFun**, el primer macrovirus con capacidades de enviar documentos infectados por correo electrónico a través de MSMail. Una nueva era había comenzado. El mensaje lucía de la siguiente forma.

Asunto: "You have GOT to read this!"
De: [direccion@servidor]
A: [dirección aleatoria tomada de la libreta de direcciones]
Adjunto: c:\doc1.doc (virus adjunto)

ShareFun estaba diseñado para trabajar sólo con MSMail y no funciona con otros clientes de correo electrónico como Eudora, Microsoft OutLook, NetscapeMail o Pegasus.

Otras iniciativas originales de este año fueron **Homer**, un gusano que se propagaba a través del protocolo FTP; y **Esperanto** fue, un virus multiplataforma desarrollado por el grupo 29A que podía infectar MS-DOS, Microsoft Windows y MacOs.

1998

En enero, Virus Bulletin comienza sus pruebas VB100 destinada a determinar la capacidad de detectar el 100 por ciento de virus en condiciones reales (*In-the-Wild*). Actualmente, VB100% es una de las certificaciones independientes más importante y respetada.

La compañía Symantec intenta afianzar su mercado con la unificación de su producto al laboratorio de IBM, al antivirus de Intel Corporation, QuarterDeck y ViruSweep.

Por su parte, NAI adquiere a Dr. Solomon's y este último desaparece de la escena antivirus, después de ser el encargado de marcar el camino.

Los virus de macro continúan expandiéndose y aparecen nuevos experimentos entre los que se puede destacar **Cross**, el primero en infectar dos aplicaciones de la familia Microsoft Office: Word y Access; y **Triplicate** (o **Tristate**) capaz de infectar Word, Excel y PowerPoint.

Aparece también **Marburg**, un virus polimórfico creado por GriYo del grupo 29A, capaz de infectar archivos ejecutables de Win32 y distribuido en los CD de algunas revistas europeas.

Otras innovaciones fueron realizadas por el grupo australiano **RedTeam**, quienes desarrollaron un virus capaz de infectar archivos ejecutables de Windows y utilizar el cliente Eudora para adjuntarse a los correos. Otra creación de este grupo fue el virus de macro **Antimarc** para Word97 que se distribuía a través del programa de chat mIRC y el cliente de correo Outlook Express. Además aparecen las primeras PoC (Prueba de Concepto) sobre virus escritos en lenguajes VBS, Java (virus **BeanHive**) y HTML.

El mismo año aparecen **BackOrifice** (del mítico grupo Culto de la Vaca Muerta o cDc por sus siglas en inglés de "the **C**ult of the **D**ead **C**ow"), **NetBus**, **Phase** y **D.I.R.T.**; cuatro troyanos que dieron que hablar marcando sin duda el inicio de actividades maliciosas de más de un adolescente. Estos programas, diseñados como herramientas de administración remota, permitían ser instalados sin conocimiento ni consentimiento del usuario, lo que desató una verdadera avalancha de instalaciones indiscriminadas en miles de equipos al tiempo que generaba controversias en igual magnitud.

Lo más destacable de este año lo logra, sin lugar a dudas, el virus de origen taiwanés llamado **CIH** (iniciales de su autor, el estudiante **Chen Ing-Hou**) o **Chernovyl** detectado en junio y activado en 26 de abril de año siguiente (aniversario del accidente en Chernobyl) o el 26 de cada mes, según la versión del virus.

Este estudiante manifestó en repetidas ocasiones que "siente mucho el daño de su creación viral, pero fue motivado por una venganza en contra de los incompetentes desarrolladores de software antivirus". Chen fue acusado de esparcir su creación y en septiembre de 2000 fue declarado culpable por la justicia de su país.

Lo que hacía a CIH tan especial era su rutina de daño diseñada para borrar los primeros 2048 sectores del disco rígido sobrescribiendo algunos tipos de Flash-Bios y dejando inutilizable la placa madre de la computadora. Otro hecho que hizo tan común a CIH fue que algunas revistas y empresas distribuyeron por error CD's infectados.

CIH revive la antigua técnica de infección creada por Tom Duff en 1989 mediante la cual las infecciones de este virus no aumentaban el tamaño de los archivos infectados, al introducir el código del virus dentro de los espacios en blanco del código de los archivos huésped.

1999

A principios de este año surge el troyano **Happy** (conocido como Ska en mención a su autor, el francés **Spanska**), estrenando una nueva moda que persiste hasta el día de la fecha: los gusanos para MS Outlook. Happy se caracteriza por su mensaje "Happy New Year 1999 !!" y sus efectos de fuegos artificiales. Debido a su capacidad de modificar ciertos archivos del sistema operativo es capaz de enviarse a sí mismo a cada persona a quien el usuario envía un correo.

El 26 de marzo **Melissa** (en memoria a una bailarina exótica) comenzó a llegar a miles de correos en un archivo adjunto enviado por alguien conocido. Este virus fue el encargado de echar por tierra un mito y un consejo que era palabra santa hasta ese momento: "no abra mensajes de personas desconocidas".

Cuando se abre el archivo adjunto con Word 97 o 2000 el virus de macro se activa, abre el Outlook, y se auto envía a los primeros cincuenta contactos de la libreta de direcciones. Estas personas reciben un documento infectado de alguien conocido y continúa la cadena de propagación. El archivo que se adjunta puede ser cualquiera que el usuario tenga en su sistema, por lo que este virus ocasiona que información confidencial salga a la luz.

Las capacidades de Melissa y la confianza del usuario en quien le enviaba el correo, hizo que este macrovirus se expandiera rápidamente y causara grandes pérdidas económicas.

Quizás debido a que el gigante del hardware (Intel) y del software (Microsoft) fueron infectados, la unidad de lucha contra el crimen cibernético de Estados Unidos buscaron y arrestaron al autor de Melissa: **David L. Smith**, un programador de Nueva Jersey de 30 años que en Mayo del 2002 fue sentenciado a 20 meses de prisión y a una multa de U$S 5.000.

En junio aparece **ZippedFiles**: un gusano que llega por correo en formato .EXE con capacidades de replicación en recursos compartidos; y dos virus conceptuales para Microsoft Windows NT: **Remote Explorer** desarrollado como un servicio en modo usuario e **Infis** primero en ejecutarse en modo Kernel.

También es digno de mención el virus **Parvo**, otro polimórfico de GriYo, capaz de infectar Windows 95, 98 y NT. Este virus implementa su propia rutina SMTP, desarrollada en Assembler. Es capaz de enviarse a múltiples direcciones de correo con sólo estar conectado a Internet. Fue uno de los primeros virus en utilizar direcciones de origen del correo falsas (spoof) para facilitar su propagación, lo que lo hace similar a los gusanos actuales.

En septiembre cae otro mito, "nadie puede infectarse con sólo leer un correo". El golpe definitivo lo da **Bubbleboy** programado en VBS que aprovechaba una vulnerabilidad en el navegador web Internet Explorer y en el cliente de correo Outlook Express.

Se inicia una nueva generación de gusanos que se propagan a través del correo electrónico sin archivos adjuntos, capaz de ingresar al sistema cuando el mensaje es abierto.

Bubbleboy, inspirado en un personaje de la serie norteamericana Seinfield, en el cual un joven vive en una burbuja provocando situaciones graciosas; fue creado por el argentino **Zulu**, explotando un agujero de seguridad descubierto, por el español **Juan Carlos García Cuartango**. Microsoft solucionó la vulnerabilidad al poco tiempo pero sin embargo el gusano siguió propagándose ya que los usuarios no actualizaban sus sistemas (esta tendencia aún permanece).

Zulu también fue el autor de otros especímenes como **Freelink**, **Monopoly**, **Stages** (un gusano muy complejo, que utilizaba el formato SHS) y **PDFworm** (primero en utilizar el formato de archivos PDF).

Por último, el 7 de diciembre aparece **Babylonia**, creado por **Vecna**, otro programador argentino radicado en Brasil. Este era un virus muy complejo y el primero en explotar la autoactualización desde Internet (muy común hoy en día).

Si bien BeanHive ya había incursionado en estas experiencias, puede decirse que Babylonia fue el primero en hacerlo eficientemente. Valiéndose de servidores ubicados en Japón era capaz de descargar una nueva versión de sí mismo. Más tarde, esta misma técnica sería empleada por **Hybris** (también conocido como sexyfun o enano) del mismo autor, con encriptación de 128 bits y capaz de instalar extensiones (plug-ins) para sí mismo.

2000

El fin del mundo informático del año 2000 no fue tal pero marcó algunos avances importantes en lo que a malware se refiere.

En este año comienza a hacerse popular un generador de gusanos, el **VBSWG** (**V**isual **B**asic **S**cript **W**orm **G**enerator). Su autor es otro argentino apodado **[K]alamar**. El mejor ejemplo de virus creado por este software es el virus **Anna Kournikova** (detectado como **SteeLee** y que llegó a infectar a la NASA), generado por el joven holandés **OnTheFly**, en agosto.

Otra noticia destacada del año fue la aparición del "gusano del amor": **LoveLetter** en Manila, Filipinas. Llegaba por correo electrónico con un archivo adjunto. Su nombre se debe a que uno de los asuntos del mensaje era "ILOVEYOU". Los daños ocasionados por este gusano se calcularon en millones de máquinas infectadas y de dólares en pérdidas.

Los principales involucrados en este caso fueron **Onel de Guzmán** de 23 años, su hermana **Irene de Guzmán** y su novio **Reonel Ramones**. Este correo dañino surgió como tesis final de Onel, la cual fue rechazada por no cumplir con los requisitos académicos de legalidad y cuyo código llegó al público infectando millones de sistemas.

Si bien algunas fuentes mencionan que una organización contrató a Onel para el desarrollo de sistemas de seguridad, él sostiene en diversas entrevistas que esto no es cierto.

Otros hechos destacables en este año fueron la aparición de PoC como:

- **Liberty**, un troyano para PalmOS, el sistema operativo de Palm Pilot de 3COM.
- **Stream**, el primer virus que hace uso de la capacidad de Microsoft Windows 2000 para dividir un archivo en Alternate Data Streams (ADS o simplemente "streams"), cuando se utiliza NTFS (New Technology File System – Sistema de archivos de Nueva Tecnología).
- **Fable**, el primer gusano de Internet implementado como un "inocente" archivo PIF (Windows Program Information).

2001

Este año estuvo marcado por la proliferación de gusanos que usan combinaciones de vulnerabilidades para su expansión, una fórmula ampliamente utilizada en la actualidad.

En los primeros días del año aparece **Pirus**, el primer virus desarrollado en lenguaje PHP y que sólo se ejecuta en servidores Web (*Nix y Windows).

En enero nace **Ramen** y en marzo **Lion**, gusanos para el sistema operativo Linux, que aprovechan diversas vulnerabilidades en RPC, wuftpd y BIND.

Durante marzo, aparece en Suecia el gusano polimórfico **Magistr** utilizando rutinas de envío SMTP propias evitando así la utilización de clientes de correo. Toma relevancia por sus ingeniosas técnicas y capacidades de propagación (generando mensajes con asuntos diferentes cada vez) y destrucción similares a CIH (eliminación de CMOS, la Flash BIOS e información almacenada en el disco).

Además de estar encriptado y tener técnicas anti-debugger, sus funciones escritas en Assembler, lo hacían difícil de detectar y eliminar. De acuerdo a su código fuente, fue desarrollado en la ciudad de Malmo, Suecia, por **The Judges Disemboweler**.

En abril aparece el peligroso gusano **BadTrans** capaz de propagarse a través del correo utilizando el Microsoft Outlook. Permite el robo de información confidencial, y su mala programación hace caer a los servidores de correo. En su segunda versión se corrigen los errores y se agrega la "funcionalidad" de ejecutar el archivo adjunto recibido, sin necesidad de que el usuario abra dicho adjunto (nuevamente valiéndose de una vulnerabilidad ya corregida).

En julio aparece **CodeRed** que se propaga buscando servidores con IIS 5.0 (Internet Information Server) vulnerables. Cuando encuentra un servidor, el gusano intenta ingresar al sistema a través del puerto 80, explotando una vulnerabilidad. Este es otro caso en donde si bien la actualización por parte de Microsoft ya existía, el gusano continuó su expansión debido a la irresponsabilidad de los administradores.

Según algunos datos estadísticos, CodeRed logró infectar 80.000 servidores en las primeras horas de la fecha de su ataque y llegó a duplicar su área de propagación cada 37 minutos. Esto sólo sería superado por **Slammer** dos años después.

También, en julio, el troyano **SirCam**, escrito en México en lenguaje Borland Delphi, es capaz de enviarse a si mismo a todos los usuarios de la libreta de direcciones de Windows, y a direcciones encontradas en los archivos temporales de Internet, además de aprovecharse de los recursos compartidos y de contener una peligrosa rutina de destrucción. La forma más común de identificarlo era su asunto en español "Hola como estas?".

En septiembre aparece el troyano **Nimda** (admin, de administrador, invertido) que se propaga por correo al visualizar páginas web, a través de recursos compartidos y atacando servidores web (ISS de Microsoft). Una consecuencia directa de la gran propagación de este gusano es la ralentización de la red, debido al gran tráfico generado buscando otros servidores vulnerables.

Aparece el virus polimórfico **Elkern** que es propagado por el gusano **Klez** (explotando las mismas vulnerabilidades que Nimda). Esta forma conjunta de actuar entre un gusano y un virus marcaría un nuevo hábito que persiste hoy en día.

Se suma una nueva forma para propagar malware: aparecen **Hello** y **Choke**, gusanos que se aprovechan del programa MSN Messenger de Microsoft para lograr su objetivo. Si bien estos conceptos ya se habían probado anteriormente en AOL Messenger, es la primera vez que aparece malware que los explota eficientemente.

En otro contexto, en mayo aparece un "gracioso" hoax (mensaje de correo de correo electrónico falso) en el que se alerta acerca que un programa (sulfnbk.exe) es un peligroso virus.

Este mensaje daba instrucciones precisas para eliminar este archivo si el mismo era hallado. El caso es que este archivo efectivamente siempre era encontrado porque pertenece a Windows. Al eliminarse, ciertas capacidades del sistema operativo dejaban de funcionar. El correo lucía de la siguiente forma:

Este VÍRUS no tiene vacuna. Lo acabo de recibir… y estaba en mi computador. Busca en tu computador el archivo: sulfnbk.exe (lo tenia en mi casa - y ya lo borre!, o sea que no puedo pasarlo de nuevo). Anda al menú iniciar, localizar (o find) y localiza este archivo y borralo imediatamente (en caso de que lo encuentres, se aloja en c:/windows/command). Después de esto borralo también de la papelera. Se trata de un vírus que viene a través de e-mails sin que te des cuenta y va a destruir tu computador el día 01.

Linux tampoco estuvo a salvo este año. Aparecen **Ramen** y **Lion**, gusanos que explotan distintas vulnerabilidades de sistemas Red Hat.

En marzo de este año también se anunciaba la aparición de **Winux**, una PoC capaz de infectar ejecutables de Windows y de Linux. Esta PoC hacía referencia al autor, Benny, y al grupo 29A.

Si de múltiples plataformas se trata, en este año también surge **Sadmind** un gusano capaz de infectar el demonio (*demon*) sadmind del sistema operativo Solaris y a servidores Microsoft IIS a través de ciertas vulnerabilidades de los mismos.

2002

En enero aparece la original PoC **LFM**, el primer virus capaz de infectar Macromedia Shockwave Flash (archivos .SWF) y programado en ActionScript. Otra PoC digna de mencionar es **Etap** (o MetaPHOR o Simile), un complejo virus metamórfico de MentalDriller (del grupo 29A), multiplataforma y sin carga destructiva como todos los de este grupo.

El día de los enamorados marca la aparición de **Yaha** (o Lentin o San Valentín) un falso protector de pantalla de San Valentín. Debido a esta técnica de engaño logró una propagación masiva.

En mayo, el gusano **Spida** comienza a aprovecharse de servidores SQL de Microsoft cuya cuenta de administrador (SA) tiene contraseña en blanco (configuración por defecto).

El descubrimiento de **Frethem** y **Bugbear** (o tanatos) marcan la aparición de malware empaquetados para evitar su detección por parte de los antivirus. En estos casos el empaquetador utilizado era UPX (**U**ltimate **P**acker for e**X**ecutables) aunque actualmente existen cientos de tipos.

El empaquetado consiste en la compresión y encriptación de un archivo ejecutable para disminuir su tamaño y cambiar su apariencia. Estas acciones no necesariamente deben ser utilizadas por programas dañinos aunque suele ser una práctica común.

Otro digno de mencionar es **Benjamín**, el primer gusano que intenta reproducirse a través de la red de intercambio de archivos formada por los usuarios de la popular aplicación Peer-to-Peer Kazaa.

También aparece **Opasoft** (u Opaserv), un gusano que se reproduce a través de recursos compartidos utilizando el puerto 139 (Netbios, NETBeui). Esta propagación la logra a través de una vulnerabilidad corregida exactamente dos años antes.

En cuanto a Linux, se crea **Slapper,** un gusano que intenta aprovecharse de la vulnerabilidad de desbordamiento de buffer en el componente OpenSSL en servidores Apache.

También aparecieron nuevos hoax similares a sulfnbk.exe del año anterior. Este fue el caso de jdbgnr.exe, sfc.exe y ace-?.

2003

El año en que un concepto antiguo vuelve a sembrar pánico en Internet. El gusano **Slammer** (o Sapphire), utilizando una vulnerabilidad del servidor Microsoft SQL (ya corregido) logró record imaginables sólo por **Nicholas C. Weaver** y su teórico gusano Warhol (ensayo donde se exploran las posibilidades de infectar el mayor número de computadoras en el menor tiempo posible).

El gusano Slammer infectó menos computadoras que CodeRed, pero actuó dos veces más rápido infectando más del 90% de las computadoras vulnerables tan sólo 10 minutos después de iniciar su propagación.

Según **CAIDA** (*Cooperative Association for Internet Data Analysis*), Slammer duplicaba su área de propagación cada 8,5 segundos, y alcanzó 55 millones de equipos rastreados por segundo en sólo 3 minutos, buscando nuevas computadoras vulnerables para infectarlas con el consecuente incremento de tráfico en la red.

En agosto de este año Microsoft comienza su programa de recompensas ofreciendo U$S 250.000 a quien entregue informes sobre creadores de virus.

En los primeros días del año se conoce **Sobig** un gusano cuyos principales aspectos a considerar, más allá del logro de su propagación (1 de cada 20 correos contenían Sobig) son su auto actualización realizada desde distintos sitios y el colapso a los que sometió a algunos servidores webs por el tráfico ocasionado por el envío de su versión F (la más propagada).

Un año después, **Author Travis Group** publicaría un informe anónimo dando detalles de este gusano y de sus presuntos autores, encabezados por el ruso **Ruslan Ibragimov**.

En agosto aparece **Mimail**, un gusano que si bien no utilizaba ninguna técnica original, logró una amplia repercusión.

La segunda epidemia fue causada por el gusano **Blaster** (o Lovesan o Msblast o Poza), que apareció en agosto aprovechando vulnerabilidades en Remote Procedure Call (RPC) de Microsoft Windows, corregidas un mes antes, para reproducirse.

El excesivo tráfico que generaba en busca de computadoras vulnerables afectó considerablemente a Internet en los días de su evolución. Contenía una rutina que intentaba conectarse a www.windowsupdate.comen una fecha determinada para ocasionar un ataque de DDoS (Distributed Denial of Service o Ataque Distribuido de Denegación de Servicio), y colapsar este servicio de Microsoft.

Con Blaster, por primera vez las recompensas de Microsoft rinden sus frutos. Un joven de 18 años, **Jeffrey Parson**, admite haber modificado el gusano original y crear una nueva versión del mismo (Blaster.B).

Las formas más comunes para identificarlo eran reinicios inesperados, errores en diversas aplicaciones de Office y, el más común, una ventana informando que el sistema se reiniciará en 60 segundos.

En este año comienzan a conocerse y a utilizarse las **botnets** (más conocidas como **redes de computadoras zombies**). Una botnet es una herramienta que puede ser utilizada con diversos fines (como el conocido proyecto SETI@home para búsqueda de vida extraterrestre), pero que actualmente han logrado su repercusión al ser utilizadas por creadores de malware para difundir sus obras dañinas. Los fines más comunes de una de estas redes son:

- Distributed Denial-of-Service Attacks (DDoS)
- Distribución de spam y phishing
- Escuchas de tráfico de red (Sniffing)
- Keylogging
- Distribución de nuevos malware
- Abuso de publicidad
- Robo masivo de datos

Los gusanos más conocidos programados para armar estas redes son **Agobot** (o Gaobot o Morphine o Phatbot o Forbot o XtremBot), **RBot** (o SDBot o UrBot o UrXBot) y **Mydoom/Mytob**, existiendo cientos de variantes de ellos y siendo modificados a diario.

La habilidad y "éxito" de estos gusanos radica en que son capaces de desactivar cualquier software de seguridad (como firewall y antivirus), explotar diversas vulnerabilidades del sistema, lograr su propagación en decenas de formas e infectar gran variedad de sistemas operativos para lograr los objetivos mencionados.

Además se comienza a hacer cada vez más popular una tendencia que se arrastra desde la aparición de los primeros códigos maliciosos. Con Internet, los virus "famosos" están al alcance de la mano y cualquier creador con "escasa inventiva" puede tomar las partes más interesantes de cualquiera de ellos y crear su propia "arma de destrucción masiva".

Según un estudio publicado por www.honeynet.org el tamaño de una botnet es variable y puede llegar hasta 50.000 equipos controlados por un solo grupo.

2004

Este año estuvo marcado por diferentes códigos maliciosos y por algunos hechos curiosos como el combate que distintos grupos desarrolladores entablan a través de sus creaciones.

En enero aparece el destructivo **Mydoom**, un gusano que se propaga por correo electrónico y la red de intercambio de archivos Kazaa, permitiendo el control remoto del equipo infectado. Más allá de esos detalles técnicos, el objetivo primario de Mydoom era hacer caer el sitio SCO (propietaria de uno de los sistemas UNIX más difundido) y Microsoft.

El éxito al hacer caer SCO, demuestra la efectividad de las redes distribuidas (zombies) para realizar ataques de denegación de servicio. Mydoom marcó la historia como el gusano de mayor y más rápida propagación de los últimos tiempos.

En este mismo mes nace una nueva amenaza: **Bagle** (o Beagle), demostrando ser el virus más persistente e "inteligente" desde la existencia de Internet. Este gusano fue objeto de un extenso estudio que puede ser descargado desde http://www.eset-la.com/threat-center/1601-historia-virus-bagle

En febrero se desata un alto porcentaje de propagación de **Netsky**, un gusano empaquetado, que contiene su propio motor SMTP, que evita enviarse a las casas antivirus y que se propaga a través de los recursos compartidos del sistema. Un detallado informe sobre este gusano puede ser consultado desde: http://www.eset-la.com/threat-center/1606-netsky-viaje-tiempo

En mayo de este año comienza a circular un gusano llamado **Sasser**, buscando sistemas Microsoft Windows 2000, 2003 y XP que aún no hayan parcheado una vulnerabilidad en el proceso LSASS (Local Security Authority Subsystem), reparada por Microsoft e informado en un boletín del mes anterior.

Debido a otra recompensa ofrecida por Microsoft (la misma cantidad que en el caso de Blaster), un estudiante alemán de 18 años (**Sven Jaschan**), fue arrestado y acusado de ser el creador de este gusano. Otras investigaciones permitieron vincular a este mismo estudiante con Netsky, previamente analizado.

Posteriormente, el adolescente declaró que su "intención original era crear un virus llamado Netsky para combatir al Mydoom y al Bagle, borrándolos de las computadoras infectadas".

En esta misma fecha, otro joven de 21 años, fue detenido en Alemania confesando haber creado junto con otras personas, el gusano Agobot previamente mencionado.

Según algunas fuentes consultadas, esto "es un claro signo del funcionamiento de la política de las recompensas".

Sin embargo, durante este año ciertas versiones de Netsky siguen propagándose, incluso ocupando los primeros lugares de los rankings.

Con respecto a otras plataformas, cabe destacar la PoC **MP3Concept**, el primer troyano para MAC OS X que, si bien no llego a extenderse, explotaba una vulnerabilidad que permitía que las aplicaciones ejecutables parezcan ser otra clase de archivos (en este caso MP3).

Comienza a hacerse popular un riesgo mencionado durante años por todos los especialistas en seguridad: la propagación sobre tecnología móvil.

El mítico grupo 29A nos entrega más de sus originales creaciones:

- **Cabir**, un gusano capaz de reproducirse a través de teléfonos móviles con el sistema operativo EPOC o Symbian (según la versión), aprovechando su posibilidad de conectarse mediante la tecnología inalámbrica Bluetooth.
- **Rugrat**, una PoC desarrollada en Assembler IA64 para demostrar el funcionamiento de virus en las nuevas plataformas Windows-Intel de 64 bits.
- **Shruggle**, una PoC desarrollada en Assembler AMD64 para demostrar el funcionamiento de virus en las nuevas plataformas Windows-AMD de 64 bits.

En agosto aparece **Brador** un troyano de origen ruso para dispositivos Pocket PC con el sistema operativo Windows CE. Este troyano es capaz de comunicarse con su autor así como de abrir un puerto para que el mismo tome control del equipo infectado.

Otros ejemplos de este tipo de amenaza móvil son **Skull** y **Mosquito** para sistemas Symbian.

2005

Prosigue una tendencia sostenida a través de los últimos 5 años: los virus tal y como los conocíamos dejan su lugar a los gusanos y troyanos encargados de armar redes de bots para obtener dinero. El "entretenimiento" de la creación de virus ya no es tal, se ha convertido en un negocio muy rentable.

Quizás la mejor prueba de ello sean los denominados **espías bankers** de los cuales se cuentan miles de variantes y cuyo principal método de propagación se basa en la modificación permanente de su código, de forma de evitar la detección de los antivirus.

Estos programas generalmente se distribuyen mediante spam y/o haciendo uso de otros malware. Se trata de troyanos que roban información relacionada con las transacciones comerciales y bancarias del usuario infectado.

La forma de funcionamiento es la misma en la mayoría de ellos: el troyano permanece en memoria monitoreando la navegación del usuario y cuando éste accede a un determinado sitio web de

instituciones financieras, captura sus datos sensibles (como nombre de usuario, contraseñas, números de tarjetas de créditos, cuentas bancarias, etc.).

En lo que se refiere a expansión de gusanos, la nota especial la puso la familia **Sober**, la cual logró una amplia repercusión desde agosto a diciembre de este año. Esta familia nació en octubre de 2003 y ha sabido mantenerse en los rankings durante todo el año.

En noviembre de este año se desata el caso Sony y su misterioso rootkit (conjunto de herramientas destinadas a modificar el sistema y ocultar su presencia) utilizado para proteger discos de música comerciales. A partir de aquí, diversos malware se aprovecharon del software instalado por la empresa para realizar otros fines.

Se conocen otras PoC de virus para móviles entre los que podemos citar a **CommWarrior** que se vale de los mensajes multimedia (MMS) para propagarse en el sistema operativo Symbian.

2006

A comienzo de este año ve la luz **Leap** un virus que afecta al sistema operativo Mac OS X y se propaga a través del programa de mensajería instantánea iChat.

Cuando todos daban a los macrovirus por desaparecidos, en junio **Stardust** daba que hablar al ser el primeros capaz de infectar macros de los paquetes OpenOffice y Staroffice en cualquiera de las plataformas en que se ejecuten los mismos.

Este año nuevamente es escenario de muchas familias de gusanos y troyanos donde es importante remarcar a **Brontok, HaxDoor, IRCBot, ExploitVML,** y **Stration** (o **Spamta**) en el último cuarto de año. Con respecto al gusano Brontok, al igual que Beagle y Netsky, también se ha realizado un informe técnico que detalla su funcionamiento, el mismo puede ser leído desde:

http://www.eset-la.com/threat-center/1604-brontok-gusano-ganador

En agosto de este mismo año, las autoridades marroquíes condenaron a prisión a dos estudiantes: **Farid Essebar** de 19 años, y **Archraf Bajloul** de 22, por su participación en la creación y difusión del gusano **Zotob**.

La popularización de juegos en línea como SecondLife (basado en el libro de ciencia ficción Snow Crash), World of Warcraft (WoW), Dark Age of Camelot, Legend of Mir (LoM), entre tantos otros, dio nacimiento a una familia de malware diseñados para obtener información sobre los perfiles de los personajes de estos juegos: **OnLineGames**, cuyo objetivo principal es obtener información de los jugadores como nombre de

usuarios, contraseñas y perfiles de los mismos. Un informe detallado sobre esta amenaza, puede ser leído en:

http://www.eset-la.com/threat-center/1788-jugando-sucio

Del mismo modo, los ataques de phishing comienzan a ser cuestiones cotidianas y surgen las primeras versiones de **Qhost**, un troyano diseñado para modificar el archivo *hosts* en cualquier sistema operativo para redireccionar al usuario hacia una página web falsa (pharming local). Se pueden ver videos sobre el funcionamiento del phishing y los troyanos del tipo Qhost en la sección de Videos Educativos de ESET Latinoamérica:

http://www.eset-la.com/threat-center/videos-educativos/

Qhost no poseen una participación relevante durante este año pero comenzará a ser amenazas latentes y de amplia difusión en los siguientes.

2007

El 2007 se caracterizó por la infinidad de códigos maliciosos creados con el objetivo de robar información confidencial de los usuarios para luego cometer diferentes acciones de índole delictiva donde los casos de phishing fueron lo más notorios.

En este aspecto, se comenzó a propagar con mayor fuerza el troyano Qhost, cuyas primeras variantes comenzaron a actuar durante el año 2006, alcanzando niveles de propagación realmente importantes.

A mediados de año, se reflotan viejas técnicas de infección a través de diferentes amenazas cuyas acciones tienen características propias de los viejos virus informáticos. Aparecen las primeras versiones de **Sality**, un virus polimórfico con capacidad de gusano capaz de infectar los archivos ejecutables que se encuentran en la computadora víctima y, en la mayoría de los casos, permite el acceso al sistema por parte del atacante de una manera no convencional (backdoor), registra toda la información que ingresa al sistema por intermedio del teclado (keylogger) y tiene la capacidad de terminar procesos de ciertos programas antivirus.

Por otro lado, renace con mayor actividad una amenaza cuyas primeras variantes surgieron al finalizar el año 2006: **Virut**, otro virus informático con capacidades polimórficas que lo tornan una amenaza muy peligrosa que, al igual que en algunas variantes de Sality, también infecta con su código archivos del tipo binarios con extensión .EXE y .SCR.

Virut se transforma rápidamente en una de las amenazas más peligrosas debido a la capacidad de mutar su código en cada infección, con lo que su eliminación se vuelve extremadamente difícil por parte de las empresas de seguridad antivirus.

La nota máxima se la llevó un gusano polimórfico llamado **Nuwar** que, si bien sus primeras versiones aparecieron durante noviembre del año 2006, no fue hasta principios de este año que comenzó a masificarse su infección.

Nuwar se caracterizó no sólo por formar una de las redes de computadoras zombies (Botnet) más importantes del año, sino que también por los innovadores métodos de engaño que empleaba para propagar cada actualización de su código dañino a través de uno de los canales de comunicación más utilizado como lo es el correo electrónico.

También fue conocido como Storm (Gusano de la Tormenta) a partir de enero de este año debido a que se diseminaba bajo el asunto "230 dead as storm batters Europe" haciendo alusión a una tormenta que supuestamente había dejado centenares de víctimas fatales en Europa.

Lo que tornó más efectivo aún a Nuwar fueron los diferentes métodos (Ingeniería Social) empleados para engañar a los usuarios aprovechando cada evento o noticia importante que lograba recorrer los medios de comunicación a nivel mundial como excusa para su propagación.

Algunos de los asuntos con los cuales se propaga esta amenaza, son los siguientes:

- Boy eats fried rat, pictures *(Niño come rata frita, fotos)*
- Arnold says I'm gay too! *(Arnold dice: yo también soy gay)*
- Obama admits extra-marital affair *(Obama admite romance extra matrimonial)*
- Son Stabbed to Death, Mother Injured *(Hijo muerto a puñaladas, madre herida)*
- Iran Executes 29 Convicts in One Day *(Iran ejecuta 29 condenados en un día)*
- Madonna admits Timberlake affair *(Madonna admite romance con Timberlake)*
- Spam King murder *(Rey del spam asesinado)*

Las primeras versiones de correos electrónicos diseminados por Nuwar contenían un enlace que generalmente era una dirección IP y que, al hacer clic sobre ella, el usuario era redireccionado hacia un sitio web malicioso con un *exploit* en un *script* ofuscado para evitar ser interpretado por los usuarios.

Bajo el mismo contexto, comienzan a masificarse aplicaciones como Mpack (no confundir con *mpack* una utilidad de línea de comando para manipular mensajes en formato MIME), Metaphisher, IcePack, FirePack, NeoExploit y otros, que son kits producidos por delincuentes, diseñados para instalarse en servidores y para explotar vulnerabilidades en sistemas con aplicaciones vulnerables.

Estas herramientas comerciales se instalan en servidores web y, a través de la modificación de cada página de los sitios atacados, se logra que los usuarios descarguen malware a su equipo, cada vez que visitan la página afectada.

El caso más renombrado durante este año fue el de Mpack modificando páginas web, y el Banco de la India, cuyo sitio web fue modificado por el grupo conocido por *Russian Bussiness Network* y cada cliente del banco que ingresaba era infectado.

Es importante destacar que estos paquetes no son malware en sí mismo sino que son programas con cierta cantidad de *scripts* y *exploits* para diferentes aplicaciones como navegadores, reproductores de sonido, o mensajeros. Estos *scripts* son instalados en el servidor web para permitir explotar vulnerabilidades en los sistemas del usuario. Luego, la explotación de estas vulnerabilidades permitirá descargar el malware propiamente dicho al equipo afectado.

Los clientes de mensajería instantánea como MSN Messenger/Windows Live Messenger, AOL Instant Messenger y Yahoo! Messenger, entre otros, representaron otro importante foco para la propagación de malware. Un informe técnico que detalla el funcionamiento de códigos maliciosos propagados a través de este vector, se pude leer desde:

http://www.eset-la.com/threat-center/1607-amigo-falso-malware-mensaje

2008

Durante este año, hubo un gran movimiento en torno a los códigos maliciosos, a punto tal de quedar en evidencia que en la actualidad representan un negocio redituable para quienes se dedican a lucrar con su creación y/o propagación.

A esta situación se le suma el fenómeno de las redes sociales, que cada día va en mayor aumento y desde la perspectiva en materia de seguridad de la información, constituyen uno de los focos de ataque más aprovechado por usuarios sin escrúpulos.

Las redes sociales como MySpace, Facebook, Twitter, Orkut y hi5 empiezan a ser cada vez más populares y en consecuencia comienzan a ver la luz los primeros códigos maliciosos que intentan explotarlas. Un artículo que habla sobre cómo interactúa este malware con el fenómeno de las redes sociales puede ser leído desde:

http://www.eset-la.com/threat-center/1722-analisis-tecnico-eset-redes-sociales

Además, no sólo se han transformado en fuentes de información donde delincuentes intentan recolectar diferente tipo de datos sino que también lo utilizan como vínculo para llegar hasta los usuarios más desprevenidos a través de falsos perfiles y desplegando todo tipo de publicidad (splog).

Durante el primer trimestre del 2008, se masifica la utilización de un tipo de malware cuyas primeras variantes fueron conocidas en el año 2006: el **Rogue**. Este malware, que se caracteriza por simular ser herramientas de seguridad, comienza a masificarse y a tomar notoriedad utilizando, en la mayoría de los casos, coberturas como programas antivirus. Generalmente responden a códigos maliciosos que bajo la excusa de eliminar todas las amenazas que se encuentran en el sistema, terminan descargando otros programas dañinos e infectando al usuario con diversa cantidad de otros malware.

Con la masificación de dispositivos de almacenamiento que se conectan a través del puerto USB (cámaras fotográficas, teléfonos celulares, iPod, PenDrivers, entre otros), se crea otro canal de ataque altamente explotado por el malware a través de un archivo *autorun.inf*, que permite su ejecución de manera automática, diseminándose por cuanto dispositivo se conecte en un equipo comprometido.

Estas amenazas reciben el nombre genérico de INF/Autorun y durante este año han obteniendo una alta tasa de propagación, sobre todo en grandes organizaciones y universidades donde se permite el uso de estos dispositivos.

Otras cuestiones importantes a destacar, son la evolución, en cuanto a la eficacia, de las técnicas de Ingeniería Social utilizadas por el gusano Nuwar debido a la diversidad de métodos empleados por este; y el surgimiento de redes avanzadas llamadas **Fast-Flux**, que consistente en la modificación continua de la estructura de sitios web maliciosos y son utilizadas para la ejecución de diferentes ataques vía web.

También se empieza a masificar otro ataque vía web llamado Drive-by-Download. Esta técnica se refiere a la inyección de código dentro del código fuente de la página vulnerada para que, cuando el usuario ingresa a la misma, sea redireccionado a otra con contenido malicioso. Para obtener información más detallada sobre el funcionamiento del Drive-by-Download puede visitar el siguiente enlace:

http://www.eset-la.com/threat-center/1792-drive-by-download-infeccion-web

En octubre y noviembre se conoce la propagación de dos gusanos muy peligrosos: Gimmiv y Conficker respectivamente, ambos propagándose a través de vulnerabilidades encontradas en plataformas Microsoft Windows, logrando un alto porcentaje de infección en pocas horas en el caso de Conficker.

Los problemas de seguridad generados por estos gusanos, dejaron nuevamente en evidencia cuan importante es mantener reglas claras en cuanto a la implementación adecuada de actualizaciones de seguridad. En el artículo llamado “La importancia de las actualizaciones” encontrará más información:

http://www.eset-la.com/threat-center/1996-importancia-actualizaciones

También a finales del año, ve la luz una peligrosa técnica de ataque llamada ClickJacking que es explotada en la mayoría de los navegadores web más importantes. En las siguientes páginas web encontrará más información sobre esta técnica:

http://www.eset-la.com/company/1983-clickjacking-nueva-tecnica-ataque-navegadores-web

Todas cuestiones que establecen una clara visión sobre el giro completo que esta dando el malware en dirección a los ataques a través de recursos que ofrece Internet y los servidores.

2009

Durante 2009 se confirmó la tendencia de los códigos maliciosos a utilizar Internet como principal plataforma de ataque y a focalizar sus esfuerzos en el rédito económico a través del malware.

Respecto a esta última característica, se acentuó la tendencia del malware a ser utilizado como medio para obtener dinero, y como servicio para cometer otros delitos de mayor envergadura propios del ciber crimen. En este contexto, se denomina Crimeware a los códigos maliciosos que poseen algún tipo de fin financiero. Puede leerse un informe completo sobre este tipo de amenaza, sus características, motivaciones y principales métodos de propagación:

http://www.eset-la.com/centro-amenazas/2219-crimeware-crimen-siglo-xxi

A pesar de haber aparecido a finales del año anterior, el gusano Conficker fue el código malicioso más preponderante durante 2009. Situado entre las tres amenazas más detectadas en todos los meses del año, según las estadísticas del sistema de ESET, ThreatSense.Net; el gusano mantuvo sus índices de propagación altos a pesar de los amplios esfuerzos de la comunidad por alertar sobre su peligrosidad. Incluso Microsoft ofreció 250.000 dólares de recompensa a quien colabore en encontrar a los creadores del gusano. La misma continuó vacante durante todo el año. En noviembre de 2009, al cumplirse un año del lanzamiento de Conficker, ESET Latinoamérica publicó un informe resumiendo las principales características del gusano:

http://www.eset-la.com/centro-amenazas/2241-conficker-numeros

Entre otros códigos maliciosos que destacaron durante 2009, Waledac fue uno de los más propagados, especialmente en el primer semestre del año. Se trata de un troyano que se propagó masivamente durante febrero, utilizando el día de San Valentín como técnica de Ingeniería Social. Posteriormente, utilizó diversas campañas para continuar infectando sistemas. El principal objetivo de Waledac es formar una red botnet dedicada, esencialmente, al envío de spam desde las computadoras de las víctimas. Se puede leer más sobre este troyano en el artículo preparado por los especialistas de ESET Latinoamérica titulado: "Waledac, el troyano enamorado":

http://www.eset-la.com/centro-amenazas/2042-waledac-troyano-enamorado

Este troyano destaca dos factores preponderantes del malware durante 2009. Por un lado, el crecimiento de las redes botnets, que proliferaron durante el año haciéndose mayor el uso de packs de administración de equipos zombis como Zeuz, ElFiesta o AdPack. Por otro lado, la Ingeniería Social continuó siendo una estrategia altamente efectiva para la propagación de amenazas, habiéndose aprovechado durante el año temáticas como la asunción del presidente de Estados Unidos (y también el Día de la Independencia de dicho país), el accidente del vuelo de Air France, la gripe A, la película Harry Potter y el fallecimiento de Michael Jackson, entre otros; para la propagación de amenazas.

También a principio de año, se realizaron varias campañas de falsos instaladores de aplicaciones, que eran utilizados para llevar a cabo un ataque de SMS Scam: cobrar al usuario un mensaje de texto de forma ilegítima para instalar una aplicación, en muchos casos falsa. También fue frecuente la aparición de diversas variantes de rogue, tendencia que continuó durante el segundo semestre del año.

Las redes sociales también fueron blanco de ataque. Luego de la aparición del gusano Koobface a principio de año, propagándose por Facebook; el mismo re apareció meses más tarde propagándose por Twitter, red social que también sufrió diversos ataques durante el año (malware, phishing, denegación de servicio) así como Hi5 o Linkedin, entre otras.

El virus Induc fue otro de los códigos maliciosos destacados. El mismo infectaba sistemas con el entorno de desarrollo Delphi, y a todos los programas compilados en los sistemas afectados, que a su vez continuaban con la propagación. De esta forma, muchos desarrolladores (y empresas de desarrollo) se encontraron con que sus propias aplicaciones poseían un virus que afectaba a sus clientes.

Previo al lanzamiento de la nueva versión del sistema operativo de Microsoft, Windows 7; luego de la publicación de la beta pública, circuló por redes peer-to-peer una versión troyanizada del sistema operativo, lo cual hacía que los usuarios afectados utilizaran un sistema infectado desde su instalación. Finalmente, sistemas operativos como GNU/Linux y Mac OS X también sufrieron ataques de malware durante el año. En el caso de GNU/Linux, el más destacado fue Psyb0t, un gusano que infectaba diversos routers que contaban con una distribución del software libre como sistema operativo. En el caso de Mac OS X, se destacó la aparición del troyano Mac/Iservice, el primero en su especie abocado a armar una red botnets de computadoras Mac infectadas. También apareció sobre fin de año el primer gusano para iPhone.

Durante 2009 los desarrolladores de malware diversificaron, propagando diversas amenazas en distintos sistemas operativos y variadas aplicaciones de Internet y sitios web; afianzando los códigos maliciosos con fines lucrativos.

2010

A lo largo del 2010 se confirmó la tendencia del crimeware buscando la realización de delitos informáticos y el mayor beneficio económico por parte de los desarrolladores de malware. Junto a esto, se destaca la aparición de ataques dirigidos y regionales en Latinoamérica, así como también un gran protagonismo de las botnet, e importante cantidad de desmantelamientos de estas redes.

En lo que respecta a los ataques dirigidos, se destacó el ataque informático a grandes empresas tecnológicas, que se dio a conocer como Operación Aurora: un ataque que buscó el robo de información de propiedad intelectual a grandes compañías. El ataque estuvo basado en la explotación de una vulnerabilidad 0-day de Internet Explorer y el uso de técnicas de Drive-by-Download.

En segundo lugar, siendo el código malicioso más importante de todo el 2010, se encuentra el gusano Stuxnet, que consistió en un malware dirigido, diseñado exclusivamente para afectar una tecnología específica. Este código malicioso fue especialmente diseñado para causar daño en sistemas SCADA, e hizo foco principalmente en productos diseñados por la empresa Siemens. Para su propagación, también hizo uso de varias vulnerabilidades críticas y otras 0-day. Stuxnet ocupó la atención de la comunidad de la Seguridad Informática, ya que sin dudas el mismo fue desarrollado por un grupo muy habilidoso de personas, con un alto conocimiento interno de los sistemas SCADA. Puede leerse un informe completo en inglés acerca de este código malicioso, sus técnicas de propagación y características principales:

http://www.eset.com/resources/white-papers/Stuxnet_Under_the_Microscope.pdf

Otro de los puntos destacados a lo largo del año es la consolidación de las botnet como una amenaza, quizá de las más importantes asociadas al mundo del malware. Entre estas se encuentra a Zeus, el panel de administración de botnet más utilizado en todo el mundo, que contó con diversas apariciones a lo largo del año, especialmente asociadas al robo de información de credenciales bancarias. También es el caso de Koobface, quien contó con varias campañas de propagación en abril, mayo y agosto; dónde finalmente surgió una nueva variante del troyano que afectó a sistemas Linux y Mac OS, siendo la primer variante multi-plataforma de esta amenaza que ya lleva más de dos años de propagación.

Junto con el gran desarrollo de las botnet, a lo largo del año se pudo apreciar la persecución a administradores de botnet y criminales asociados al negocio delictivo, lo que conllevó al desmantelamiento de varias de estas redes. En la primer parte del año, se dieron de baja las redes conocidas como Mariposa y Waledac. En la segunda parte del año se sumó el desmantelamiento de Bredolab, la botnet que llegó a infectar a más de 30 millones de sistemas durante sus dos años de vida, así como también fueron dados de baja algunos de los centros de comando y control de Koobface.

Por otro lado, durante el año aumentaron la cantidad de ataques regionales en Latinoamérica. Estos fueron asociados principalmente a las redes de equipos zombis, como la botnet detectada en México,

conocida como Mariachi Botnet y en otra con origen en Argentina. Sucesos importantes como el terremoto en Chile o el caso de los mineros en el mismo país, o la situación política de Venezuela, llevaron al uso de técnicas de Ingeniería Social para la propagación de malware en la región.

Finalmente, también ocurrieron distintos casos de amenazas para diversas plataformas, como el caso de Mac OS y Linux. Los dispositivos móviles presentaron nuevos tipos de amenazas, especialmente las primeras variantes para algunos sistemas operativos en crecimiento, como es el caso de Android que tuvo su primer troyano SMS.

El 2010 fue un año muy activo en términos de ataques informáticos, con amenazas para diversas plataformas, una creciente incidencia de las botnet y la aparición de nuevos códigos maliciosos novedosos, así como también la continuidad de algunas amenazas que llevan años en propagación.

2011

El 2011 resultó ser un año interesante desde el punto de vista de la complejidad de algunos códigos maliciosos, como también por el auspicioso crecimiento que ha experimentado el mercado de los teléfonos inteligentes y la madurez alcanzada por el crimeware y los delitos informáticos. Los dispositivos móviles han ido evolucionando. Si bien en un principio sólo cumplían funciones básicas como llamadas o mensajes, en la actualidad, son verdaderas computadoras móviles cuyas características son cada vez más apetecidas por los ciberdelincuentes, quienes están al tanto de cómo los usuarios almacenan información confidencial o realizan transacciones bancarias.

Si a la complejidad y fenómeno de los dispositivos móviles móvil le sumamos las redes botnets, podemos armar un panorama claro de lo que fue el año 2011 en materia de seguridad informática.

Años anteriores, se pudo observar un sostenido aumento en la producción de códigos maliciosos con fines netamente económicos, es decir, que buscan obtener ganancias ilícitas mediante la usurpación de información confidencial y bancaria del usuario. En el 2011 pudimos apreciar cómo las botnet pusieron fin al malware estático, el que era programado masivamente para realizar acciones determinadas en su estructura interna, para dar paso a las amenazas dinámicas capaces de convertir un dispositivo informático en zombi, el que luego se conecta a un servidor central (botnet), quedando a merced de las órdenes que puedan determinar los cibercriminales mediante una consola de administración.

Así es como a comienzos de 2011 apareció un nuevo bootkit, Win32/Olmasco, cuyas características son el producto de la evolución de TDL4 o Win32/Olmarik. En vez de parchar el código del MBR (Sector de Arranque Maestro), modifica la tabla de partición del disco, lo que dificulta su detección y remoción del sistema, con el fin que este código malicioso permanezca inadvertido la mayor cantidad de tiempo posible en el sistema.

También aparecieron otras amenazas complejas como Win32/Sirefef que, a pesar de no ser un bootkit, es capaz de ocultar sus acciones y la información de su configuración dentro de un archivo oculto de sistema y actuar como un controlador de sistema y filtro. Por su lado, Rovnix logró establecer una tendencia que marcaría el resto del año, modificar la VBR (Volume Boot Record) y el código de Bootsrap. Ésto dificulta aún más remover este malware del sistema. Además, debido al paulatino pero progresivo crecimiento de las plataformas de 64 bit, estos bootkit y algunos rootkit también están empezando a ser compatibles con la arquitectura x64 y dicha edición de Microsoft Windows.

No contentos con lograr el control de una computadora en el proceso de carga del sistema operativo, los creadores de estos bootkit fueron más allá al desarrollar uno (Win32/Mebromi) capaz de infectar el BIOS del sistema dificultando su desinfección, al extremo de poder necesitar, en algunos casos, un cambio en el chip CMOS del sistema afectado.

Toda esta complejidad observada en estos códigos maliciosos que tienen como objetivo principal convertir las computadoras en zombi, deja en evidencia que los ciberdelincuentes siempre están en una búsqueda constante por mejorar y ampliar sus técnicas de ocultamiento con el fin de seguir obteniendo ganancias ilícitas la mayor cantidad de tiempo posible. Más información sobre el funcionamiento de estas amenazas puede ser consultada en nuestro artículo "Evolución de los bootkit en el 2011".

Respecto del fenómeno móvil, y pese a que a principios de 2011 sólo aparecieron siete variantes para Android, durante la mitad del año comenzó a cimentarse una tendencia que probablemente será observada con aún más fuerza en el presente año: el crecimiento constante de malware para dispositivos móviles destinado principalmente al sistema operativo Android. Esto se explica debido a la alta penetración que han logrado los teléfonos inteligentes, habiendo más de 5 mil millones de dispositivos móviles en el mundo, de los cuales alrededor de 500 millones están repartidos en varios países de Latinoamérica.

Según estudios de Gartner, a mediados de 2011 Google contaba con un 43% de la cuota de mercado de sistemas operativos móviles lo que obviamente resulta atractivo para las bandas de ciberdelincuentes que actualmente concentran parte de sus recursos en la creación de este tipo de códigos maliciosos. Así, durante la mitad del año aparecieron 29 familias de malware para Android, de las cuales un 60% resultaron ser amenazas con alguna característica propia de una botnet, o sea, que el dispositivo queda a la espera de instrucciones remotas, convirtiéndolo en un verdadero "zombi móvil".

En 2011 los cibercriminales responsables de las prolíferas redes zombis Zeus y SpyEye lograron cubrir todo el mercado de sistemas operativos móviles con sus adaptaciones ZITMO y SPYTMO respectivamente. Aunque desde septiembre de 2010 ya existían versiones de Zeus para Symbian y BlackBerry, casi un año más tarde esa lista pasó a incluir otras alternativas como Windows Mobile y Android. Lo mismo sucedió con SpyEye, cuyas ediciones mobile aparecieron por primera vez y de a poco durante el transcurso de 2011. Nuestro artículo sobre Tendencias 2012 detalla más al respecto.

Otro hito importante del año fue Win32/Dorkbot, gusano que apareció en abril, pero que obtuvo su primer encuentro con la fama cuando en julio logró posicionarse en el séptimo lugar dentro de los códigos maliciosos más detectados a nivel mundial, y tercero en Latinoamérica según nuestro sistema de alerta temprana ThreatSense.Net®. El mes de septiembre fue el período en el cual la variante Dorkbot.D logró posicionarse como la amenaza con mayor prevalencia en nuestra región con un 10,14% del total de las detecciones, relegando a INF/Autorun a un segundo lugar y a Conficker a una quinta posición. Los tres países más afectados por Dorkbot han sido México, Perú y Colombia.

Respecto a la parte técnica, esta familia de gusanos está compuesta por cuatro variantes principales, las que utilizan dispositivos de almacenamiento masivo USB como principal vector de expansión para lograr establecer una amplia red de computadoras zombi, volviendo a remarcar la madurez que obtuvo el crimeware o, en otras palabras, malware creado específicamente para cometer delitos informáticos. También remarcar que desde la variante B, este gusano aparte de enviarse mediante Windows Live Messenger también lo hace por Facebook.

Respecto de la masificación en el uso de redes sociales durante el año era de esperarse que características como la inmediatez en la información o el alto impacto que transmiten medios como Facebook, y en especial Twitter, fueran aprovechadas por los cibercriminales como canal de envío para expandir malware y realizar estafas. Como en la mayoría de los casos, estas campañas de propagación de amenazas tienen mayor éxito en base a la originalidad que tengan las tácticas de Ingeniería Social que se empleen.

En el mes de agosto apareció un troyano bautizado por ESET como Win32/Delf.QCZ. Aparte de fingir ser el antivirus que la víctima tenga instalado en su sistema, este código malicioso intenta expandirse a través del chat de Facebook simulando ser una persona real que conversa con el usuario antes de enviar el hipervínculo malicioso. Este enlace hace alusión a un supuesto video “sensacional” que incluye el nombre de la cuenta del individuo para hacerlo parecer más legítimo.

Finalmente cabe señalar que durante 2011 aparecieron algunas amenazas para Mac y Linux destinadas a lograr establecer una botnet cuyos zombis sean sistemas operativos UNIX. Aunque, por lo general, suelen no tener el mismo nivel de producción y complejidad que para Windows o Android. En este sentido los troyanos Linux/Tsunami y OSX/Tsunami representan un acercamiento al mundo de las botnets al ser códigos maliciosos que permiten transformar a equipos zombis las computadoras que utilicen esas plataformas.