

CONTENIDO

Prólogo	xxi
Acerca de los autores	xxv
Agradecimientos	xxix
Introducción	xxx
PARTE I. EL PROBLEMA	1
Capítulo 1 Definiciones básicas	3
Virus informáticos, hechos y fantasías	4
Definiciones	5
Virus y mecanismos de virus	6
Estructura de un virus	6
Daño	7
Daño versus infección	8
Mecanismos de ocultación	8
Polimorfismo	9
¿Qué es esto, un libro de UNIX?	9
Dieta de gusanos (worms)	11
Troyanos	11
En libertad (In the wild)	12
Guía rápida de software antivirus	13
Resumen	14
Capítulo 2 Revisión histórica	17
Prehistoria de los virus: de Jurassic Park a Xerox PARC .	18
Agujeros de gusano (WormHoles)	18

Core Wars	19
El gusano de Xerox (Gusano de segmento de Shoch y Hupp)	20
Virus reales: primeros días	21
1981: Primeros virus de Apple II	22
1983: Elk Cloner	22
1984: Fred Cohen. Virus informáticos. Teoría y experimentos	23
1986: © Brain	24
1987: Buenas noches Vienna, Hola Lehigh	25
1988: El gusano Turns	27
La era de Internet	29
1989: Gusanos, Dark Avenger y AIDS	29
1990: Polimórficos y multipartitos	31
1991: Virus del Renacimiento, Tequila Sunrise	32
1992: La venganza de la tortuga	33
1993: Triunfa el polimorfismo	35
1994: Smoke me a kipper	36
1995: Virus de macro de Microsoft Office	37
1996: Macs, macros, el universo y todo	38
1997: Hoax y correos en cadena	38
1998: No es una broma	39
1999: Aquí llega la decimonovena vez que se te funde el servidor	39
2000: Año del gusano/virus de VBScript	42
Y continúa...	46
Resumen	47
Capítulo 3 Malware definido	49
Qué hacen las computadoras	50
Funcionalidad vírica	51
Funcionalidad de aplicación frente a la seguridad	51
In the wild frente a cantidades terriblemente altas	52
¿Qué detectan los antivirus actualmente?	54
Virus	56
Gusanos	58
Intenciones	59
Corrupciones	60
Gérmenes	60
Droppers	60
Virus de prueba	61
Generadores	62
Troyanos	62
Robo de claves y puertas traseras	65
Jokes (Bromas)	67
Herramientas de acceso remoto (RATS, Remote Access Tools)	69

Agentes DDoS	70
Rootkits	71
Falsas alarmas	72
Resumen	73

Capítulo 4 Funcionamiento y actividad viral **75**

¿Cómo se escribe un virus?	77
Estructura tripartita	80
Mecanismos de infección	80
Detonante (trigger)	81
Payload o carga	82
Replicación	83
Virus no residentes	84
Virus residentes en memoria	84
Virus híbridos	85
Generalidad, alcance, persistencia	85
Payload contra reproducción	87
Daño	88
Impacto de las infecciones virales en el entorno informático	88
Daño directo causado por los payloads de virus y troyanos	89
Daño psicológico y social	90
Daño secundario	90
Daños al hardware	91
Evita la bomba	92
Bombas lógicas	92
Bombas de tiempo	92
Bombas ANSI	92
Bombas de correo y bombas de suscripción	93
Resumen	94

Capítulo 5 Mecanismos de virus **95**

Virus para hardware específico	96
Virus de sector de arranque	97
La zona de arranque	101
Virus que infectan archivos	103
Prependers and Appenders	105
Virus de sobrescritura	106
Redirección	108
Virus de compañía (Replicantes)	109
Virus multipartitos	110
Virus interpretados	112
Virus de macro	112

28/11/11

7182

tema

x *Contenido*

Virus de script	114
Mecanismos de ocultación	114
Ocultamiento	117
Polimorfismo	120
Ingeniería social y malware (Código malicioso)	122
Resumen	125
PARTE II. SOLUCIONES DE SISTEMA	127
Capítulo 6 Vistazo a la tecnología contra código malicioso	129
Grandes expectativas	130
¿Cómo nos las vemos con los virus y otras amenazas?	132
Medidas preventivas	133
¿Qué hace un programa antivirus?	140
Más allá de la computadora personal	149
Outsourcing	156
Resumen	157
Capítulo 7 Gestión del malware	159
Definiendo la gestión del malware	160
Gestión proactiva	161
Gestión reactiva	171
Costes de la propiedad frente a los costes de administración	173
Resumen	177
Capítulo 8 Recogiendo información	179
¿Cómo comprobar si el aviso es auténtico o provechoso?	180
Libros	182
Los buenos	183
Los malos (o al menos los mediocres)	183
Los verdaderamente desagradables	184
Cuestiones relacionadas	186
Seguridad general	186
Legal	189
Ética	190
Ficción	190
Artículos y escritos	192
Recursos online	198
Listas de correo y grupos de noticias	199
Escáneres gratuitos	200
Escáneres online	201

Enciclopedias	201
Bulos sobre virus y falsas alertas	202
Evaluaciones y comparativas	203
Creadores de antivirus	203
Recursos generales	204
Artículos varios	205
Advertencias generales	206
Vulnerabilidades y virus específicos	206
Referencias generales sobre seguridad	209
Capítulo 9 Evaluación del producto y prueba	215
Principales aspectos	216
Coste	217
Rendimiento	222
No es mi configuración por defecto	228
Desinfección y reparación	230
Aspectos de la compatibilidad	232
Rango funcional	233
Sencillez de uso	238
Posibilidades de configuración	239
Comprobabilidad	240
Funciones de soporte	240
Documentación	244
Servicios delegados a terceros	245
Prueba comparativa	245
Detección contra uso	246
Otras clasificaciones	246
Actualización	247
Está ocurriendo todo en el «zoo»	249
Nos gusta EICAR	253
Más información	256
Resumen	256
Capítulo 10 Gestión de riesgos e incidentes	257
Gestión de riesgos	259
La mejor forma de defensa es la preparación	260
La computadora	260
La oficina	262
Mantenimiento preventivo	264
Lo primero, no perjudicar	267
Informes de incidentes con virus	268
Investigaciones de la oficina de soporte	269

Tratando incidentes víricos	270
Identificación vírica	272
Políticas generales de protección	272
Resumen	273
Capítulo 11 Gestión del usuario	275
Gestionando a los gestores	276
Las políticas cuentan	277
Seguridad y seguros	278
Virus y seguros	278
Análisis riesgo/impacto	278
Costes de gestión	280
Políticas	282
Soporte ofrecido por la Oficina de Soporte	283
Otro personal de soporte de IT	286
Seguridad de IT y otras unidades	286
Preparación y educación	287
Refuerzo positivo	290
Gestión preactiva de software malicioso	291
Directrices sobre conjuros de seguridad	291
Contrastar todas las alertas con el departamento de IT	291
No se debe confiar en los adjuntos	292
Cuidado en los grupos de noticias y en la web	293
No instalar programas no autorizados	293
Cautela con los documentos de Microsoft Office	294
Utilizar y pedir formatos de archivo más seguros	294
Hay que seguir usando el software antivirus	294
Hay que mantener el software antivirus al día	295
Que esté al día no significa que sea invulnerable	295
Los súper usuarios no son superhumanos	295
Desactivar el arranque desde la disquetera	295
Disquetes protegidos contra escritura	296
Evitar Office	296
Reconsiderar el software de correo y de noticias	296
Mostrar todas las extensiones de archivos en el Explorador de Windows	297
Inhabilitar Windows Script Host	297
Poner visualización genérica de correo electrónico	297
Utilizar recursos de seguridad de Microsoft	298
Suscribirse a listas de proveedores de antivirus	298
Escanearlo todo	298
No confiarse por tener software antivirus	299
Copias de seguridad, copias de seguridad, copias de seguridad	299
Gestión de bulos	300

Formulario de respuesta	300
Guía rápida sobre bulos	301
Resumen	303
PARTE III. CASOS DE ESTUDIO: ¿QUÉ SE HIZO MAL? ¿QUÉ SE HIZO BIEN?	
¿QUÉ PODEMOS APRENDER?	305
Capítulo 12 Casos de estudio: la primera oleada	307
Brainwashing (Lavado de cerebro)	308
¿Quién creó el virus Brain?	309
Banks of the Ohio	310
El virus MacMag	311
Una oportunidad para la paz	312
La semilla abandonada	313
Las macros confunden tu mente	314
Scores	315
Leginh	317
CHRISTMA EXEC	318
The Morris Worm (Gusano de Internet)	319
El gusano WANK	322
Jerusalem	323
El troyano «AIDS»	325
Todos deben quedarse petrificados	326
Michelangelo, Monkey y otras variantes del Stoned	327
No hagas el mono con el MBR	331
Form	333
El hoax (bulo) del virus módem	334
El virus iraquí Printer	335
Resumen	338
Capítulo 13 Casos de estudio: la segunda oleada	339
The Black Baron	341
Good Times	342
El texto es lo interesante	343
Soplo en el viento	343
Rizar el rizo	343
Big Bang	343
La confirmación del virus Concept	345
Programas versus datos	345
El nombre del juego	346
¿Cuándo un payload no es un payload?	348
Automacros	350

El Imperio contraataca (lentamente)	350
WM/Nuclear	351
Colors	354
DMV	355
Wiederoffnen y FormatC	355
Green Stripe y Wazzu	356
WM/Atom	356
WM/Cap	357
Virus de Excel	357
Variaciones sobre el tema	359
Word 97	359
Gracias por compartir	361
Nomenclatura de virus de macro	361
Técnicas antimacro	362
Hare	364
Chernobyl (CIH.Spacefiller)	365
Esperanto	366
Resumen	367
Capítulo 14 Casos de estudio: llegamos a los gusanos (la tercera oleada) .	369
El gusano Autostart	370
W97M/Melissa (Mailissa)	371
Considerar su método	372
Infección frente a dispersión	373
Sans Souci	373
El virus comercial	374
Solía quererla (pero ahora, ¿está en todas partes?)	375
W32/Happy99 (Ska), el virus con valor añadido	376
PrettyPark	376
Cuidado con los virus de Script	377
VBS/Freelink	378
Escribir una carta a mi amor VBS/Loveletter	379
VBS/NewLove-A	381
¡Llama al 911!	382
VBS/Stages	383
Bubbleboy y KAKworm	384
MTX (Con la excusa de Matrix)	385
Naked Wife	388
W32/Navidad	389
W32/Hybris	390
VBS/VBSWG.J@mm (Anna Kournikova)	391
VBS/Staple.a@mm	392
Gusanos de Linux	393

Ramen	393
Linux/Lion	393
Linux/Adore (Linux/Red)	394
Lindose (Winux)	394
W32/Magistr@mm	395
BadTrans	396
Resumen	397
PARTE IV. ASPECTO SOCIAL	399
Capítulo 15 Origen y distribución de los virus	401
¿Quién escribe esto?	403
Ingeniería social	404
Definiciones de ingeniería social	406
Ladrones de claves	409
Esta vez es personal	410
¿Por qué escriben esto?	411
Distribución secundaria	415
¿La formación funciona?	416
Formación global	418
Resumen	419
Capítulo 16 Metavirus, hoax y otros conceptos relacionados	421
Cartas en cadena	423
Hoax	424
Leyendas urbanas	425
Cartas en cadena y hoax	426
Hoax y alertas de virus	426
La desinformación bajo el microscopio	428
BIOS, CMOS y pilas eléctricas	428
El hoax JPEG	429
El virus Budget	430
Un duro despertar	430
Trigo y cáscara	431
Normas de identificación de hoax	432
Spam, spam, spam (parte 2)	440
Motivaciones	440
Temas comunes	442
Spamología y virología	443
Metavirus y gestión de usuarios	444
¿Qué debería decir a mis clientes?	445
Manejarse con spam, cartas en cadena y alertas de hoax	446
Resumen	447

Capítulo 17 Imperativos legales y cuasilegales	449
El software malicioso y la ley	450
Bases para procedimientos criminales	451
Decreto sobre el mal uso informático	453
Algunos conceptos generales	454
Legislación sobre la protección de información	454
Principios sobre la protección de información	456
BS7799 y control de virus	458
ISO 9000	461
Arquitectura de la seguridad	462
¿Quién es el responsable de la seguridad en un determinado contexto? ..	466
¿Qué sistemas están protegidos?	466
¿Cuáles son los detalles de ejecución y configuración?	466
Proyecto de política	468
Uso aceptable de instalaciones y recursos	468
Uso aceptable del correo electrónico	468
Política en contra del correo encadenado	471
Política en contra del correo basura	471
Uso aceptable de la World Wide Web y USENET	472
Política sobre antivirus	472
Resumen	474
Capítulo 18 Responsabilidad, moralidad y ética	475
Guía breve de ética	476
Demografía	479
Edad	479
Sexo	481
Normas culturales y nacionales	482
Cuestiones nacionales	482
Factores motivadores	486
Diferencias entre naciones	486
Familiaridad y ética	487
El usuario final y su responsabilidad	488
¿Es la gestión antivirus una profesión?	490
Los vendedores y la ética	491
Ética comercial	493
No hagas daño	494
El desarrollo de códigos de conducta	495
Un código de conducta mínimo	495
EICAR	496
Artículo 1: Interés público	497
Artículo 2: Adecuación de la Ley	497

Artículo 3: Deber para con los empleadores, patronos, empresarios, clientes y compañeros de trabajo	497
Artículo 4: Deber para con la profesión	498
Artículo 5: Competencia en la especialidad	498
¿Son los códigos de conducta efectivos?	498
Resumen	501
Capítulo 19 Conclusión	505
Predicciones	506
Comentarios finales	507
Malas noticias: los especialistas en seguridad no saben mucho sobre virus	507
Buenas noticias: un poco de formación y unas políticas básicas pueden ayudar	508
Malas noticias: la convergencia empeora las cosas	509
Buenas noticias: más de lo mismo	510
Malas noticias: un ataque desde varios frentes puede aumentar el problema	510
Buenas noticias: utilizar las herramientas actuales con precaución puede resultar efectivo	511
Últimas publicaciones	511
RTF no es una panacea	512
Poly/Noped	513
Mandragore	514
Hoax SULFNBK	514
Sadmind	515
Cheese	515
Lindose/Winux	516
MacSimpsons	516
Outlook View Control	516
Code Red/Bady	517
Sircam	518
Resumen	519
PARTE V. APÉNDICES	522
A. Las preguntas más frecuentes de VIRUS-L/comp.virus	523
Principales aportaciones	524
¿Cuáles son los virus conocidos?	524
¿Dónde puedo obtener más información sobre virus y temas relacionados?	525
¿Qué son los virus informáticos?	526
¿Qué es un gusano?	528
¿Qué es un caballo de Troya (troyano)?	528
¿Cuáles son los indicadores de una infección vírica?	528

¿Qué pasos se deberían dar para diagnosticar e identificar a los virus? . . .	529
¿Cuál es el mejor modo de eliminar un virus?	530
¿Qué son los «falsos positivos» y los «falsos negativos»?	531
¿Podría un programa antivirus estar ya infectado?	533
¿Dónde puedo conseguir un escáner de virus para mi sistema UNIX? . . .	534
¿Por qué mi escáner solo avisa algunas veces de que hay una infección? .	535
Creo que he detectado un nuevo virus, ¿qué puedo hacer?	535
CHKDSK informa de unos 639 KB (o menos) de memoria en un sistema DOS. ¿Estoy infectado?	535
Tengo un bucle infinito de subdirectorios en mi disco duro. ¿Estoy infectado?	536
¿Puede un PC que no se ejecute en modo DOS estar infectado por un virus típico de DOS?	537
El sistema de archivos del disco duro ha sido alterado. ¿Tengo un virus? .	538
¿Es posible proteger un equipo utilizando solo software?	538
¿Es posible proteger el disco duro utilizando solo software?	539
¿Qué se puede hacer teniendo solo protección del hardware?	539
¿Nos protege de los virus el establecer los atributos de un archivo de solo lectura?	540
¿Protegen mis archivos de virus los sistemas de control de acceso o las contraseñas?	540
¿Funcionan los sistemas de protección de DR DOS frente a los virus? . . .	541
¿Utilizar una pestaña de protección contra escritura en los disquetes, detiene los virus?	541
¿Ayudan las redes locales (LAN) a detener los virus o facilitan su propagación?	542
¿Cuál es el mejor modo de hacer copias de seguridad?	542
¿Pueden los virus del sector de arranque infectar los virus de DOS que no son de arranque?	545
¿Puede esconderse un virus en la memoria CMOS de un PC?	546
¿Puede un virus de PC ocultarse en la memoria RAM expandida o extendida del PC?	546
¿Puede un virus ocultarse en la memoria superior o en la zona alta de memoria?	547
¿Puede un virus infectar los ficheros de datos?	547
¿Pueden extenderse los virus de un tipo de computadora a otra?	548
¿Las computadoras de tipo mainframe son susceptibles de contraer virus?	548
Hay quien dice que desinfectar no es una buena idea. ¿Es cierto?	550
¿Puedo evitar los virus si no utilizo shareware, freeware (software gratuito) o juegos?	551
¿Puedo contraer un virus en mi PC ejecutando el comando DIR en un disco infectado?	551
¿Puede haber algún riesgo al copiar los ficheros de datos de un disco infectado al disco duro limpio de un PC?	552

¿Puede un virus de DOS sobrevivir y propagarse en un sistema OS/2 utilizando el sistema de ficheros HPFS? 553

Bajo OS/2 2.0+, podría una sesión DOS infectada, infectar otra sesión del DOS? 553

¿Pueden los virus normales de DOS funcionar bajo MS Windows? 553

¿Puedo contagiarme con un virus leyendo los correos electrónicos? 554

¿Puede un virus «ocultarse» en un fichero .GIF o .JPEG? 555

¿Con qué frecuencia deberíamos actualizar las herramientas antivirus? 555

¿Es posible utilizar un virus informático para algo útil? 556

¿No sería una buena idea añadir el código de búsqueda a los programas? ... 557

¿Está mi disco infectado con el virus Stoned? 557

Me he infectado a la vez con el Stoned y el Michelangelo. ¿Por qué no arranca mi equipo? 558

Me he infectado con el Flip y ahora gran parte del disco duro parece haber desaparecido. ¿Qué ha ocurrido? 559

¿Qué hacen los virus GenB y/o GenP? 559

¿Cómo «arranco desde un disco limpio»? 560

El servicio de diagnóstico de mi PC incluye al «Cascade» entre las interrupciones del hardware (IRQ). ¿Significa eso que tengo un virus Cascade? 561

Cuando ejecuto DIRIMORE, veo dos ficheros con nombres distintos que no aparecen cuando solo ejecuto DIR. No aparecen en el sistema de un amigo. ¿Tengo un virus? 561

B. Los virus y el Macintosh 563

¿Cuántos virus afectan a Macintosh? 564

Virus específicos de Mac 564

 Virus que infectan los archivos y sistemas específicos de Mac 565

 Virus de Hypercard 567

 Los troyanos del Mac 568

 Virus de macro, troyanos y otros variantes 569

Virus en emulaciones de PC 571

Esperanto 4733 571

Virus PC scripting 571

 Welcome datacomp 571

El fichero de prueba de instalación EICAR 572

Fuentes de información 572

 Publicaciones relativas al Mac 572

 Bibliografía 573

 Sitios web 574

 Virus Bulletin 574

 Fuentes de información sobre virus de macro 575

 Otras fuentes sobre virus 575

Resolución de problemas de Mac	576
Preguntas recibidas en Mac Virus	576
C. Ingeniería social	581
Seguridad de IT	582
Lo que el intruso quiere saber	583
Pirateando a la gente	584
Curioseando	584
Escuchas/vigilancia	584
Acceso no autorizado	584
Ser sociable	585
Llamadas falsas	585
Rebuscando en la basura	585
Material electrónico desechado	585
Objetivo: el Help Desk (Centro de ayuda al usuario)	586
Ataques al Help Desk	586
¿Necesito revelar mi contraseña?	587
¿Notaría si alguien mostrara un interés inusitado por los sistemas de seguridad?	587
¿Cómo de grande es el riesgo?	587
¿Cuáles son las soluciones?	587
¿Cómo utilizar bien la contraseña?	589
¿Por qué es importante saber utilizar las contraseñas?	589
Contraseñas: una buena forma de reforzar los sistemas	590
Prácticas recomendables	590
¿Dónde puedo conseguir más información?	591
Glosario	593
Índice	615