

# Índice

<b>Declaración de intenciones (o por qué creo que este libro te puede interesar) .....</b>	<b>13</b>
<b>Preliminares.....</b>	<b>15</b>
<b>Introducción .....</b>	<b>17</b>
<b>Capítulo I</b>	
<b>Qué fue de los virus (hasta los troyanos bancarios).....</b>	<b>19</b>
<b>1. Qué malware fue el más importante a principios de siglo .....</b>	<b>25</b>
AnnaKournikova .....	25
Sysid .....	27
Icecubes.....	27
Sircam .....	27
Hybris.....	28
Req .....	29
PDFWorm.....	30
Magistr .....	30
Mimail.....	31
Stream .....	32
Donut.....	33
Setiri.....	34
Sobig .....	34
Zotob y Mytob.....	36
NetSky.....	36
<b>2. Qué eran los bulos de email.....</b>	<b>37</b>
Nostradamus.....	37
Sulfnbk.exe, Jdbgmgr.exe y Setdebug.exe.....	38
<b>3. Qué fue de los primeros troyanos.....</b>	<b>39</b>

Cain & Abel.....	39
Sub7.....	40
NetBus.....	41
Back Orifice .....	41
Lovgate.....	42
QAZ.....	42
Fizzer.....	43
<b>4. Qué fue de los gusanos .....</b>	<b>44</b>
Gusanos automáticos en cliente .....	44
Gusanos automáticos en servidores .....	55

## Capítulo II

### Qué fue de los troyanos bancarios

#### (hasta el ransomware).....95

<b>1. Técnicas de los troyanos bancarios .....</b>	<b>99</b>
Captura de imágenes y vídeos.....	99
Inyección en la red .....	102
Inyección en el navegador.....	102
Pharming local .....	106
Delephant .....	109
FormGrabbers .....	111
<b>2. Grandes troyanos bancarios de la época.....</b>	<b>112</b>
Beagle como ejemplo de la transición .....	112
Goldun .....	116
Phishing kits .....	116
Zeus .....	118
SpyEye .....	123
Citadel .....	127
Carberp.....	131
Zlob .....	131
Storm Worm .....	132
Torpig/Sinowal/Mebroot.....	133
Carbanak y los cajeros .....	135
Grandoreiro, Mekotio, Janeleiro ... ..	137
El navegador, protegido a toda costa .....	140

## Capítulo III

### Por qué la ciberguerra.....145

Ciberataques a Estonia .....	146
Stuxnet.....	147

FinFisher .....	150
Hacking Team .....	152
Duqu.....	153
TheFlame.....	154
Careto (The Mask) .....	159
Operación aurora.....	163
TajMahal .....	164
APTs.....	164

## Capítulo IV

### De dónde viene el malware

<b>(y cómo se distribuye) .....</b>	<b>167</b>
Los dialers .....	169
Ingeniería social .....	170
Java y PDF .....	175
Malware de macro.....	177
AutoRun y AutoPlay .....	188
Kits: MPack, BlackHole.....	189
AppStores y otros métodos móviles.....	194

## Capítulo V

### ¿El malware es solo para Windows? .....

<b>1. Malware para Macintosh.....</b>	<b>202</b>
MP3Concept.....	203
Inqtana-A.....	203
OSX/RSPug y OSX/Pupe .....	204
HellRTS.....	205
Roguewares.....	205
Shlayer.....	207
Un Kattana falso.....	208
El antivirus para Mac, xProtect.....	208
<b>2. Malware para Linux .....</b>	<b>211</b>
Ramen .....	212
Adore Worm.....	212
Santy.A .....	213
Lupper/Lupii .....	213
Linux.Encoder.1 .....	214
El día que Linus Torvalds parcheó el kernel para favorecer los virus multiplataforma.....	214
<b>3. Malware para móviles.....</b>	<b>216</b>
Pre-symbian y Symbian .....	216

Android .....	220
Malware para iPhone.....	259

## Capítulo VI

<b>Cómo se distribuye el malware .....</b>	<b>263</b>
1. Scareware y rogueware .....	263
2. Minar criptomonedas.....	266
3. Spyware, Adware y troyanos clic .....	266
4. Botnets .....	268
5. Ransomware.....	273
6. Supply chain.....	300
SolarWinds Orion.....	303
SITA, lo desconocido .....	305

## Capítulo VII

<b>Cómo se defiende y esconde el malware.....</b>	<b>307</b>
1. <b>Cómo se defiende el malware en local .....</b>	<b>307</b>
Empacado y ofuscación.....	307
Rootkits .....	308
Sistemas antidebug.....	310
2. <b>Cómo se defiende el malware en la red.....</b>	<b>311</b>
FastFlux.....	311
DGA .....	312
Bullet Proof.....	314

## Capítulo VIII

<b>Cómo nos defendemos del malware .....</b>	<b>317</b>
1. Las actualizaciones .....	318
2. Antiexploits .....	320
En el principio fue EMET .....	320
Windows Defender Exploit Guard: Exploit Protection.....	321
SMEP y SMAP.....	328
3. El cortafuegos .....	329
4. Los antivirus .....	331
Publicidad absurda .....	331
El incidente Kaspersky.....	335

---

Microsoft entra en juego .....	337
¿Por qué solo los antivirus?.....	341
<b>5. Bounty programs .....</b>	<b>345</b>
<b>6. Con la ley .....</b>	<b>347</b>
<b>7. El sentido común .....</b>	<b>349</b>
<b>Despedida y cierre .....</b>	<b>353</b>
<b>Índice de imágenes .....</b>	<b>355</b>
<b>Índice alfabético .....</b>	<b>363</b>
<b>Otros libros publicados.....</b>	<b>365</b>

