

kniha první

Počítačové viry z pohledu laika a mírně pokročilého uživatele

kapitola 1	Definice a základní vlastnosti počítačového viru	5
kapitola 2	Počítačový virus a operační systém	9
2.1.	Virus a MS-DOS	10
2.2.	Virus a Windows	11
2.2.1.	Viry v prostředí Windows 95	12
2.2.2.	Viry v prostředí Windows NT	14
2.3.	Virus a UNIX	14
2.3.1.	Morrisův červ - listopad 1988	14
2.4.	Virus a jiné operační systémy	17
2.5.	Problémy (ne)destruktivity virů	18
kapitola 3	Dělení počítačových virů	21
3.1.	Viry podle umístění v paměti	22
3.1.1.	Nerezidentní viry	22
3.1.2.	Rezidentní viry	23
3.2.	Viry podle cíle infekce	24
3.2.1.	Bootovací viry	25
3.2.2.	Souborové viry	29
3.2.3.	Multipartitní viry	33
3.3.	Viry podle koncepce návrhu a projevů chování	34
3.3.1.	Stealth viry	34
3.3.2.	Polymorfní viry	35
3.3.3.	Tunelující viry	38
3.3.4.	Generické viry	39
3.3.5.	Generátory virů	39

kapitola 4	Virům podobné počítačové hrozby	43
4.1.	Trojské koně	44
4.2.	Makro-viry	44
4.3.	Červi	47
4.4.	Bomby	48
4.5.	Krypto-viry jako budoucí směr vývoje?	48
kapitola 5	Virová etika a pohnutky tvůrců virů	51
kapitola 6	Základní antivirové prostředky a mechanismy	57
6.1.	Softwarové prostředky	58
6.1.1.	Jednouúčelové programy	60
6.1.2.	Programové balíky	61
6.1.3.	Informační programy	63
6.2.	Prostředky s podporou hardware	69
6.3.	Neuronové sítě a viry	70
kapitola 7	Metodické uživatelské postupy antivirové kontroly a ochrany	73
7.1.	Příznaky přítomnosti viru na počítači	74
7.2.	Základní odvírovací praktiky	79
7.3.	Základní bezpečnostní praktiky	82
kapitola 8	Počítačové viry a Internet	87
8.1.	Potenciální možnosti virového útoku	88
8.2.	Informační zdroje a (anti)virově zaměřené servery	89
8.2.1.	USENET (newsgroup) a diskusní konference (e-mail)	89
8.2.2.	Virově zaměřené textové dokumenty (FAQ, RFC)	90
8.2.3.	Anonymní FTP servery	92
8.2.4.	World Wide Web (WWW)	92

knihá druhá

Počítačové viry z pohledu programátora – virologa

kapitola 1	Programová podpora pro práci s viry	103
kapitola 2	Nejfrekventovanější virová přerušení	111
2.1.	Volání BIOSu a dokumentovaných služeb DOSu	112
2.2.	Použití nedokumentovaného DOSu	120
kapitola 3	Obecné virové mechanismy	123
3.1.	Zjištění přítomnosti viru v paměti	124
3.2.	Zjištění přítomnosti viru v souboru	125
3.3.	Zjištění adresy viru v paměti	127
3.4.	Přesměrování vektorů přerušení na tělo viru	127
3.5.	Rezidentní instalace	129
3.5.1.	Rezidentnost bootovacích virů	129
3.5.2.	Rezidentnost souborových virů	130
3.6.	Obsluha kritické chyby DOSu	136
3.7.	Charakteristické okamžiky infekce virem	136
3.8.	Typický mechanismus infekce souborových virů	138
3.9.	Simulace zavedení operačního systému	139
kapitola 4	Základní virové konstrukce	143
4.1.	Konstrukce bootovacího viru	144
4.2.	Konstrukce souborového COM viru	152
4.3.	Konstrukce souborového EXE viru	157
4.4.	Konstrukce souborového SYS viru	163

4.5.	Konstrukce souborového duplicitního viru	173
4.6.	Konstrukce polymorfních virů	176
4.6.1.	Princip implementace polymorfismu	176
4.6.2.	Generátor pseudonáhodných čísel	178
4.6.3.	Semi-polymorfní reverzibilní algoritmus	179
4.6.4.	Polymorfní reverzibilní algoritmus	180
4.6.5.	Polymorfní nereverzibilní algoritmus	183
4.7.	Konstrukce stealth virů	185
4.8.	Konstrukce tunelujících virů	187
4.9.	Konstrukce Windows virů	191
4.10.	Konstrukce generátorů virů	197
4.11.	Konstrukce makro-viru	199
kapitola 5	Obranné virové mechanismy	201
5.1.	Pasivní obrana	202
5.2.	Aktivní obrana	202
5.2.1.	Přesměrování ladících přerušení	203
5.2.2.	Obrana pomocí časovače	204
5.2.3.	Skládání kódu	205
5.2.4.	Využití fronty instrukcí	207
5.2.5.	Vypnutí rezidentních antivirových hlídačů	208
<hr/>		
	Slovníček pojmů	211
	Rejstřík	215