Diffusione dei virus in Italia

Presentiamo questo mese un'analisi ragionata della diffusione dei virus nel nostro paese durante l'anno 1995.

di **Gianfranco Tonello** (tge@maya.dei.unipd.it)

Per realizzare quest'analisi abbiamo osservato un campione costituito sia da utenza aziendale che privata, difficilmente quantificabile in termini numerici. Le segnalazioni sono state comunicate spontaneamente, principalmente per mezzo di telefax, ma anche grazie a mezzi telematici quali le reti Fidonet ed Internet. Pertanto è ipotizzabile che le cifre di seguito commentate e le statistiche ricavate siano sottostimate, ma certamente in grado di dare un quadro reale e significativo del fenomeno della diffusione dei virus in Italia.

Tipi di virus

Si è rilevata, dopo accurata analisi ed elaborazione delle segnalazioni, una conferma della situazione già segnalata in I.V.M. (Italian Virus Magazine n. 01 Aprile 1995) per il 1994. Quell'anno furono riscontrati i Italia cinquanta virus distinti, mentre nel 1995 sono passati a sessantaquattro, quindi con un incremento di circa il 22%. Questi dati contrastano in modo sostanziale con notizie apparse su quotidiani a livello nazionale, che a più riprese hanno asserito che i virus prodotti nel mondo ogni mese sono oltre 200. Alcune fonti stimano in oltre settemila i virus noti fino ad ora, ma come si può vedere probabilmente questi non si trovano tutti circolanti in Italia. Sarebbe interessante approfondire questo "dettaglio", ma soprattutto capire a chi giova tutto ciò. Si può comunque arguire che è solo una scorretta questione di "immagine" il dichiarare pubblicamente, di riconoscere mille virus più di qualunque altro software antivirus.

Proseguiamo la nostra analisi limitata all'Italia, che certo rispetto alle catastrofi informatiche tanto agognate all'estero, sembra essere un'isola "felice", sebbene la pirateria (una delle pratiche di maggior rischio per la diffusione dei virus) sia ancora molto diffusa sia a livello privato che aziendale.

Dall'elenco dei virus circolanti, tra i primi dieci ne troviamo ben quattro di origine italiana, quali Invisible_Man.2926, RPS2, November_17th.900.C e Marzia.D.

La novità di rilievo riguarda il virus RPS2 noto dal febbraio 1995. Questo agente patogeno colpisce l'MBR (Master Boot Record) degli hard disk e il Boot Sector dei floppy disk, dopo quaranta boot della macchina va a riscrivere alcuni settori chiave del disco fisso rendendolo inaccessibile.

In terza posizione è da segnalare l'HLLC.Crawen.8306, caratterizzato dall'essere un codice virale di tipo gemellare.

In prima posizione vi è la conferma del virus Junkie.1027, che è stato diffuso in Italia nel settembre 1994 attraverso un floppy allegato ad una rivista informatica. All'epoca il codice virale non veniva riconosciuto da alcun antivirus (questo a parziale scusante dei diffusori). Purtroppo, anche nel 1995 non è mancato un caso analogo riguardante il virus Bye, anch'esso distribuito su un floppy disk allegato ad una rivista informatica. In quest'ultimo caso però il virus era già noto in Italia dal mese di maggio, ed era già disponibile un software antivirus liberamente utilizzabile (freeware) che lo intercettava. Sarebbe bastato usarlo per evitare la diffusione dell'agente patogeno nel nostro Paese. Come si può vedere dalla tabella 1, il virus Bye è già in nona posizione sebbene sia diffuso massicciamente solo da novembre 1995 (tabella 1).

Virus italiani e stranieri

Come si può vedere dalle tabelle riportate, i virus segnalati attivi in Italia nel 1995 sono stati sessantaquattro, dei quali venticinque sono stati creati da autori italiani (o che si "firmano" tali) mentre trentanove sono codici virali "stranieri" o almeno così sembra dall'analisi del codice virale, ma che hanno avuto modo di produrre infezioni anche nel nostro paese. Dagli elenchi nelle tabelle due e tre, risulta che il 30% delle infezioni rilevate sono state prodotte da virus di origine italiana, mentre il 70% è stata originata da virus "stranieri".

Dall'analisi dell'elenco dei codici virali stranieri, si rileva, che molti di questi sono virus di "recente generazione" come il Junkie.1027, il B1 e l'HLLC.-Crawen.8306 etc., questi codici virali vengono riconosciuti solo dagli antivirus che hanno avuto un aggiornamento recente (non è il caso di MSAV, anti-virus fornito di serie nelle versioni di MS DOS Microsoft a partire dalla versione 6.0) (tabella 2 e 3).

I virus più resistenti

Si sono dimostrati virus più resistenti quelli che si installano nel Boot Sector e/o Master Boot Record (MBR), i quali sono i più "tranquilli"; infatti dopo l'installazione nel Boot Sector e/o MBR dei dischi fissi operano l'infezione continua di tutti i dischetti inseriti.

Non trasmettendosi attraverso i file, e

Tabella 1- Lista delle infezioni nel 1995:

Nome Virus	N. casi	%
01) Junkie.1027	279	20,17%
02) Form	123	8,89%
03) HLLC.Crawen.8306	114	8,24%
04) B1	91	6,57%
05) Invisible_Man.2926	87	6,50%
06) RPS2	75	5,42%
07) November_17th.900.C	61	4,41%
08) Marzia.D	52	3,75%
09) Bye	43	3,10%
10) AntiExe	41	2,96%
11) Boot.446	40	2,89%
12) November_17th.855.A	31	2,24%
13) Flip.2153.A	25	1,80%
14) Parity_Boot.B	24	1,73%
15) Arianna.3375	18	1,30%
16) Die_Hard	17	1,22%
17) Barrotes.1310	16	1,15%
18) Run_Error_504D:5658	16	1,15%
19) Cascade.1701.A	15	1,08%
20) One_Half.3544	15	1,08%
21) Ripper	14	1,01%
22) Yeke.1204	13	0,93%
23) Bloody_Warrior	12	0,86%
24) November_17th.900.B	11	0,79%
25) Italy	10	0,72%
26) HLLC.Crawen.8516	10	0,72%
27) Rebelbase	9	0,65%
28) HDKiller	9	0,65%
29) Tequila	8	0,57%
30) Jumper.B	6	0,43%
31) Bravo	6	0,43%
32) Jerusalem.1244	5	0,36%
33) Fax_Free.1536.Topo	5	0,36%
34) Kampana.A	5	0,36%
35) Star_Dot.789.A	5	0,36%
36) TaiPan.438	5	0,36%
37) Hidenowt	4	0,28%
38) November_17th.768.A	4	0,28%
39) November_17th.1007	4	0,28%
40) Gullich	4	0,28%
41) Quox	4	0,28%
42) V-Sign	4	0,28%
43) New_ExeBug	4	0,28%
44) Polifemo.736	4	0,28%
45) Ping_Pong	4	0,28%
46) November_17th.800.A	3	0,21%
47) Stoned.Angelina	3	0,21%
48) Yeke.1076	2	0,14%
49) November_17th.768.B	2	0,14%
50) November_17th.706.B	2	0,14%
51) November_17th.998	2	0,14%
52) Natas.4744	2	0,14%
53) Gippo.Epidemicware.1242	1	0,07%
54) SHOO.2803	1	0,07%
55) Stoned.Swiss	1	0,07%
56) Gippo.JumpingJack	1	0,07%
57) November_17th.880	1	0,07%
58) _1360	1	0,07%
59) Stoned.Empire.Monkey.B	1	0,07%
60) Jerusalem.998	1	0,07%
61) Stoned.HiDos	1	0,07%
62) Milano	1	0,07%
63) Vota_DC.591	1	0,07%
64) V2PX.1260	1	0,07%
TOTALE INFEZIONI	1383	

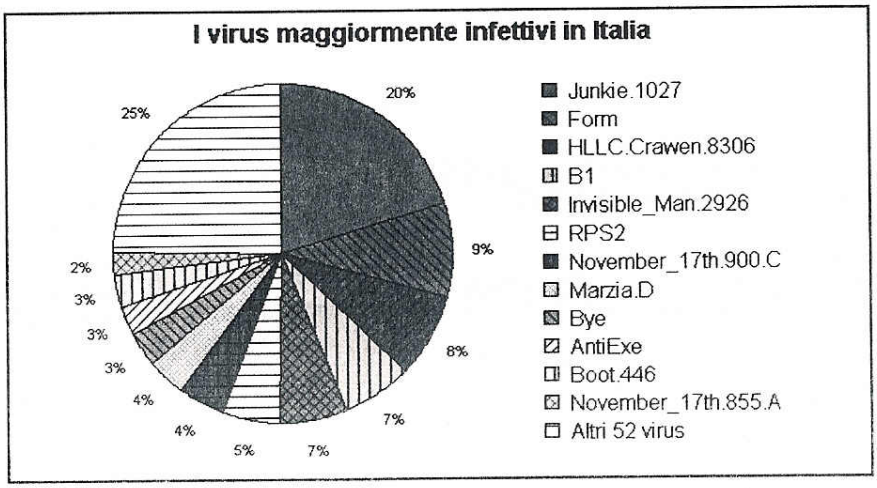
Tabella 2

Virus Italiani	N. Casi
01) Invisible_Man.2926	90
02) RPS2	75
03) November_17th.900.C	61
04) Marzia.D	52
05) November_17th.855.A	31
06) Arianna.3375	18
07) Bloody_Warrior	12
08) November_17th.900.B	11
09) Rebelbase	9
10) Bravo	6
11) Fax_Free.1536.Topo	5
12) Star_Dot.789.A	5
13) November_17th.768.A	4
14) November_17th.1007	4
15) Gullich	4
16) Polifemo.736	4
17) Ping_Pong	4
18) November_17th.800.A	3
19) November_17th.768.B	2
20) November_17th.706.B	2
21) November_17th.998	2
22) Gippo.Epidemicware.1242	1
23) Gippo.JumpingJack	1
24) November_17th.880	1
25) Vota_DC.591	1
TOTALE casi di infezione	408

quindi non allungandoli di dimensione, non producono segn "visibili" della loro azione e il computer, nella maggior parte de casi, continua a funzionare in modo apparentemente corretto Dall'elenco dei virus soprattutto stranieri si può vedere che quell di Boot sono rappresentati in maniera consistente e sono soprat tutto virus di recente generazione quali il B1, Bye, AntiExe Boot.446 ma anche virus endemici come il Form. Dopo i virus che infettano "solamente" il Boot, troviamo nelle prime posizion

Tabella 3

Virus Stranieri	N. Casi
01) Junkie.1027	279
02) Form	123
03) HLLC.Crawen.8306	114
04) B1	91
05) Bye	43
06) AntiExe	41
07) Boot.446	40
08) Flip.2153.A	25
09) Parity_Boot.B	24
10) Die_Hard	17
11) Barrotes.1310	16
12) Run_Error_504D:5658	16
13) Cascade.1701.A	15
14) One_Half.3544	15
15) Ripper	14
16) Yeke.1204	13
17) Italy	10
18) HLLC.Crawen.8516	10
19) HDKiller	9
20) Tequila	8
21) Jumper.B	6
22) Jerusalem.1244	5
23) Kampana.A	5
24) TaiPan.438	5
25) Hidenowt	4
26) Quox	4
27) V-Sign	4
28) New_ExeBug	4
29) Stoned.Angelina	3
30) Yeke.1076	2
31) Natas.4744	2
32) SHOO.2803	1
33) Stoned.Swiss	1
34) _1360	1
35) Stoned.Empire.Monkey.B	1
36) Jerusalem.998	1
37) Stoned.HiDos	1
38) Milano	1
39) V2PX.1260	1
TOTALE casi di infezione	975



virus fast infection (infezione veloce), multipartiti quali Junkie.1027, Invisible_Man.2926 e Marzia.D. Nelle prime 10 posizioni troviamo 2 virus che si trasmettono "solamente" attraverso i files (HLLC.-Crawen.8306 e November_17th.900.C), i rimanenti si trasmettono sia attraverso i files che attraverso il BOOT SECTOR e/o l'MBR (Junkie.1027, Invisble_Man.2926, Marzia.D), oppure solamente attraverso il Boot Sector (Form, B1, RPS2, Bye e AntiExe). I virus ad infezioni multipartita hanno la caratteristica di trasmettersi sia attraverso i files che attraverso il boot sector e/o l'MBR (Master Boot Record) degli Hard Disk.

È questa loro particolarità, cioè quella di fondere insieme le peculiarità delle prime due categorie di virus discusse, che li rende maggiormente aggressivi rispetto ai precedenti (tabella 4).

Conclusioni

Da quanto esposto, risulta chiaro come i Virus multipartiti siano quelli che hanno maggiore diffusione, pur avendo generato meno infezioni rispetto ai codici virali del boot sector. Questi ultimi sono però in numero maggiore rispetto ai multipartiti (ventidue virus del boot sector contro otto virus multipartiti). Sebbene i codici multipartiti siano ancora in numero limitato, se i viruswriters continueranno a produrli, e questa sembra essere la tendenza, potrebbero arrivare a creare danni anche ingenti su scala nazionale ed internazionale. Gli autori di virus "italiani", o considerati tali, sembrano maggiormente portati alla produzione di file virus, ma nel 1995 si è notato che l'interesse di alcuni si è spostata verso i Virus multipartiti. Degli otto Virus multipartiti circolanti in Italia, ben tre possono essere imputati ad autori italiani (Arianna.3375, Invisible_-Man.2926, Marzia.D).

Alla comunità informatica italiana e mondiale non resta che sperare che questi

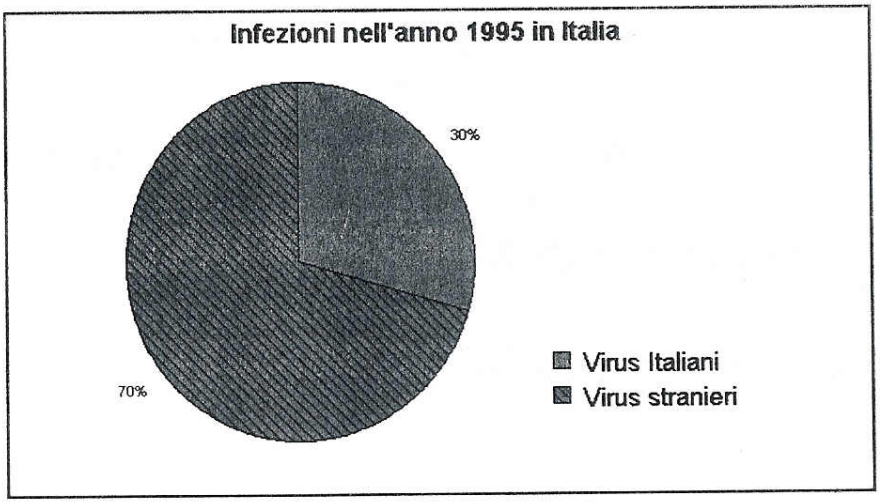
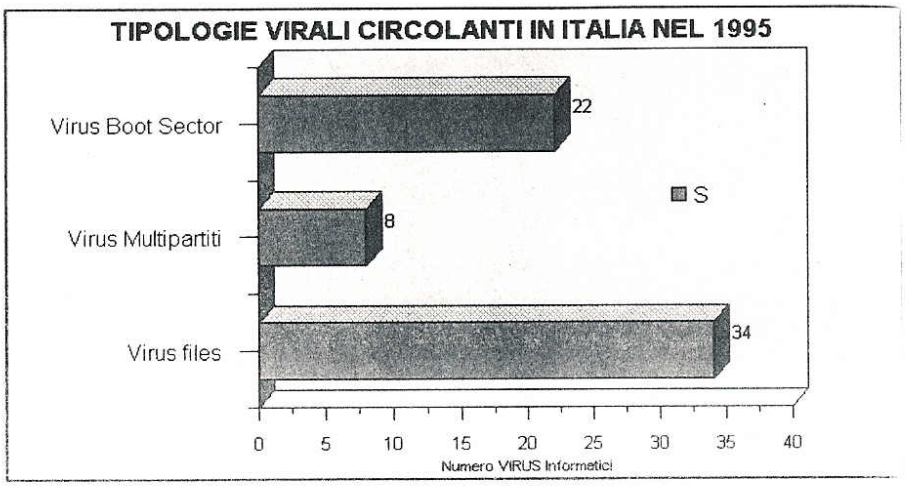


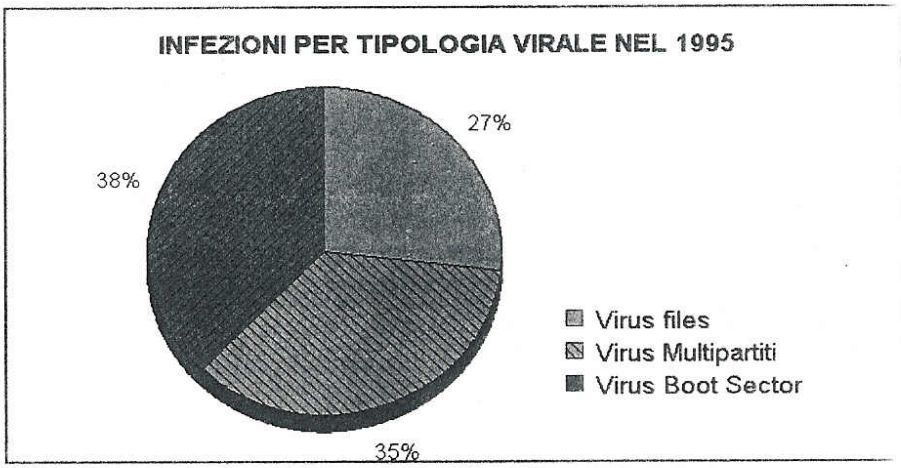
Tabella 4

Virus dei files	N. casi
01) HLLC.Crawen.8306	114
02) November_17th.900.C	61
03) November_17th.855.A	31
04) Die_Hard	17
05) Barrotes.1310	16
06) Cascade.1701.A	15
07) Yeke.1204	13
08) Bloody_Warrior	12
09) November_17th.900.B	11
10) HLLC.Crawen.8516	10
11) Rebelbase	9
12) Bravo	6
13) TaiPan.438	5
14) Star_Dot.789.A	5
15) Jerusalem.1244	5
16) Fax_Free.1536.Topo	5
17) Polifemo.736	4
18) November_17th.768.A	4
19) Hidenowt	4
20) November_17th.1007	4
21) November_17th.800.A	3
22) November_17th.768.B	2
23) November_17th.706.B	2
24) November_17th.998	2
25) Yeke.1076	2
26) SHOO.2803	1
27) Gippo.JumpingJack	1
28) _1360	1
29) November_17th.880	1
30) Gippo.Epidemicware.1242	1
31) Jerusalem.998	1
32) Milano	1
33) Vota_DC.591	1
34) V2PX.1260	1
TOTALE casi di infezione	371

VIRUS DEL BOOT SECTOR	N. casi
01) Form	123
02) B1	91
03) RPS2	75
04) Bye	43
05) AntiExe	41
06) Boot.446	40
07) Parity_Boot.B	24
08) Run_Error_504D:5658	16
09) Ripper	14
10) Italy	10
11) HDKiller	9
12) Jumper.B	6
13) Kampana.A	5
14) New_ExeBug	4
15) V-Sign	4
16) Quox	4
17) Ping_Pong	4
18) Gullich	4
19) Stoned.Angelina	3
20) Stoned.HiDos	1
21) Stoned.Empire.Monkey.B	1
22) Stoned.Swiss	1
TOTALE casi di infezione	523

Virus MULTIPARTITI	N. casi
01) Junkie.1027	279
02) Invisible_Man.2926	90
03) Marzia.D	52
04) Flip.2153.A	25
05) Arianna.3375	18
06) One_Half.3544	15
07) Tequila	8
08) Natas.4744	2
TOTALE casi di infezione	489





fantomatici personaggi (dalle capacità no certo comuni) si ravvedano e spostino i loro interesse verso programmi di mag giore utilità sociale. Per quanto ci riguar da, non ci resta, che essere atten all'osservazione del fenomeno Virus, con fidando soprattutto nella collaborazion dell'intera comunità informatica, la qual ad ogni ritrovamento di codice viral dovrebbe operare la sua segnalazione e eventualmente l'invio di campioni pe l'analisi, permettendo ai ricercatori anti virus di mettere a punto apposite contromisure per combatterli.

Gianfranco Tonello è ricercatore antivirus e sviluppatore del pacchetto antivirus VirITPro, disponibile anche in versione freeware chiamata VirIT Lite.