Italian VIRUS Magazine

LA PRIMA RIVISTA ITALIANA DEDICATA ALLA LOTTA ANTI-VIRALE MS-DOS

Trimestrale - Anno 1, 1/95 Aprile 1995

Italian VIRUS Magazine

Italian VIRUS Magazine è una rivista elettronica dedicata alla lotta antivirale con particolare attenzione alla realtà italiana, con l'obiettivo di sensibilizzare la comunità informatica verso gli agenti patogeni che ogni giorno tentano di insidiare i nostri calcolatori e quindi il nostro prezioso lavoro.
IVM è gratuita, quindi liberamente copiabile e distribuibile senza scopo di lucro.
Le informazioni riportate possono essere utilizzate totalmente o parzialmente da chiunque, senza chiederne preventiva autorizzazione, con il solo obbligo di citarne la fonte:
"TG Soft - Il Servizio Anti-Virus italiano - (Tel. 049-631748)"

Hanno collaborato: Gianfranco Tonello, Enrico Tonello, Fabrizio Toniolo

Via Sardegna n° 5
35030 Sarmeola di Rubano (PD)
Tel. 049-631748

NEWS

RPS2 colpisce Brescia

Sono giunte numerose segnalazioni relative alla diffusione del virus RPS2 nella provincia di Brescia. Il codice virale infetta il boot sector dei floppy e il master boot record del disco fisso, risulta essere pericoloso perchè può sovrascrivere con valori casuali i settori dell'hard disk.

The Virus Creation 2000 System by Havoc The Chaos

Questo è un nuovo programma progettato per la realizzazione di codici virali. Il suo funzionamento è molto semplice, anche persone non molto esperte in materia, sarebbero in grado di generare nuovi codici virale. Di seguito riportiamo uno stralcio integrale della documentazione, nel prossimo numero di IVM vi sarà un articolo appronfondito sull'argomento.

```
What VC2000 Is:
==============

        The Virus Creation 2000 System (VC2000), is a virus   creator designed for complex code
generation, great configurability, and ease of use.   There is only one file   that you need,
VC2000.EXE (which is presently under 22k). After asking   you a   series of   questions, it will then
create a MASM/TASM compatible assembly   source code   of your virus, along with a
"MAKEVIR.BAT" which helps   speed things along a bit.   Another great option, is the   virus
detector, which you can custom configure.   This will trap an interrupt, and when the virus calls the
interrupt with DX equaling what you set it for, it will warn you and give you an option to halt the
program.
```

Polifemo.736 trovato a Roma

E' stato ritrovata una variante del virus POLIFEMO, di origine italiana. Il virus è molto attivo nella città di Roma.

Rapporto sulla diffusione in Italia nel 1994

di Enrico Tonello

Il campione osservato

Il campione osservato è costituito sia da utenza aziendale che privata quantificabili in 20.000 (ventimila) e più computer monitorati, i quali utilizzando il software da noi prodotto VirIT e VirIT Lite spontaneamente hanno segnalato per lo più a mezzo telefono, ma anche grazie a mezzi telematici quali la rete amatoriale FIDO Net (Gianfranco Tonello 2:333/316.4) e la rete internazionale INTERNET (tge@maya.dei.unipd.it) i virus dei quali loro malgrado erano rimasti vittime. Sono stati inserite anche segnalazioni avute attraverso software quali SCAN McAfee, VDS, ed F-Prot, sebbene in molti casi, per lo meno per i primi 2 l'erronea e nella maggior parte dei casi mancato riconoscimento esatto della variante non ha permesso di avere dati attendibili. A tale proposito invitiamo i lettori del presente rapporto di utilizzare VirIT Lite per il monitoraggio delle infezioni in Italia, per almeno 2 motivi: 1) il software è gratuito di libera distribuzione (non a scopo di lucro) 2) ha la capacità di intercettare le varianti, grazie alla metodologia reticolare di implementazione delle FIRME di riconoscimento, con ottima precisione.

Da quanto detto è ipotizzabile che le cifre di seguito commentate e le statistiche ricavate siano sottostimate, ma certamente in grado di dare un quadro reale del fenomeno.

Dove trovare VirIT Lite

software FREEWARE di monitoraggio dei virus circolanti in Italia

1) Presso il sito FTP del D.S.I. dell'Università di Milano ftp.dsi.unimi.it nella directory pub/security/docs/TGSoft, con il nome VLT-***.ZIP
2) Presso tutte le BBS della rete VIRNET sempre con il nome già citato
3) Presso GREENEYES CBCS (Tel. 049-8800998, 24h/24 fino a 14.400)
4) Presso tutti i distributori di programmi "GO GO Soft"

Tipi di virus circolanti in Italia

Si è rilevato, dopo accurato studio dei campioni, una inversione di tendenza rispetto agli anni precedenti. Mentre negli anni scorsi i virus più diffusi erano codici virali di vecchia generazione quali FORM, Flip e Cascade, virus stranieri che grazie alle inesistenti contromisure preventive ed alla novità assoluta del fenomeno hanno avuto modo di proliferare ed essere ritrovati nella più svariate località dell'intero "globo terrestre", nel 1994 i virus più diffusi sono stati virus di produzione italiana, cioè fatti da autori italiani, i quali hanno avuto per lo più diffusione zonale, nazionale nel caso dell'Invisible_Man.2926, regionale ed a volte ancora più ristretta provinciale o poco più come nel caso del Vota_DC.591 (Padova).
Nasce da questa interpretazione fenomenologica la necessità non tanto della prevenzione verso tutti i virus circolanti nel mondo, ma una prevenzione mirata verso quelli realmente presenti nel territorio, i quali originano per lo più infezioni a livello locale, e per questo motivo vengono snobbati e/o tardivamente inserite (ammesso che campioni degli stessi vengano mandati agli sviluppatori dei software stranieri) da parte dei produttori di anti-virus stranieri i quali debbono badare per lo più a mantenere aggiornato il loro Dbase di FIRME virali verso i codici virali dove risulta essere più diffusa la loro clientela (U.S.A. ed Inghilterra).

N.	Nome Virus	N° Inf.	%
01	Yankee_Dooble.Wobble	861	49,62%
02	Junkie.1027	173	9,97%
03	Arianna.3375	95	5,48%
04	Form	72	4,15%
05	B1	45	2,59%
06	Invisible_Man.2926	43	2,48%
07	Topa.2456	35	2,02%
08	Vota_DC.591	31	1,79%
09	November_17th.900.C	30	1,73%
10	November_17th.998	29	1,67%
11	RebelBase	27	1,56%
12	Datalock	23	1,33%
13	November_17th.800.A	21	1,21%
14	November_17th.800.B	19	1,10%
15	November_17th.900.B	18	1,04%
16	Gippo.EpidemicWare	15	0,86%
17	GoldBug	13	0,75%
18	Yeke.1204	13	0,75%
19	November_17th.855.A	12	0,69%
20	Tai-Pan	12	0,69%
21	November_17th.768	12	0,69%
22	November_17th.1007	12	0,69%

23	Jerusalem.1808.Standard	9	0,52%
24	Marzia.D	9	0,52%
25	Ping_Pong	8	0,46%
26	HLLC.Crawen.8306	6	0,35%
27	Lubec_II.1135	6	0,35%
28	Lubec_II.736	6	0,35%
29	AntiExe	6	0,35%
30	Dir_II	6	0,35%
31	Gullich	6	0,35%
32	Gippo.Stunnig_Blow	5	0,29%
33	Marzia.C	5	0,29%
34	Cascade.1704	5	0,29%
35	StarDot.801	5	0,29%
36	HLLC.Crawen.8515	4	0,23%
37	Marzia.B	4	0,23%
38	Gippo.JumpingJack	4	0,23%
39	V-Sign	4	0,23%
40	Polifemo.906	4	0,23%
41	Italy	3	0,17%
42	Ripper	3	0,17%
43	Keypress.1232.A	3	0,17%
44	Parity_Boot.A	3	0,17%
45	_571	2	0,12%
46	Stoned	2	0,12%
47	Run_error_504D:5658	2	0,12%
48	Michelangelo	2	0,12%
49	Yankee_Doodle.44	1	0,06%
50	Brain.Ashar	1	0,06%
T O T A L E		1735	100%

Come si può notare quasi il 50% delle infezioni segnalate sono da imputare ad un solo virus il Yankee_Dooble.Wobble noto anche con il nome "Casteggi" perché la prima segnalazione è venuta nei primi mesi del 1993 dalla città di Casteggio (PV). La diffusione di questo codice virale è imputabile non tanto a particolarità del virus, il quale per altro non è che un codice virale derivato dal "vecchio" Yankee Doodle al quale è stata aggiunta una routine che lo crittografa, quanto alla diffusione da parte di un'azienda produttrice di applicativi per il sistema bancario dell'aggiornamento di un programma per la gestione dei cambia valute. Questo aggiornamento è stato inviato a 150 tra centri consortili e banche le quali ignare che il software celasse al suo interno questa sgradita sorpresa l'hanno utilizzato. Il problema è stato brillantemente risolto grazie alla immediata segnalazione dell'infezione in atto ed all'invio immediato del software VirIT personalizzato per la rimozione dello sgradito ospite.

Junkie.1027 è il secondo virus più diffuso in Italia, la sua diffusione è certamente legata ad un dischetto contenente un demo di un videogioco, il

quale oltre a questo conteneva nel settore di BOOT dello stesso il virus Junkie.1027. In questa occasione vi fu un forte clamore soprattutto da parte di vari quotidiani a diffusione nazionale, che, forse consigliati da "esperti" e/o presunti tali, ricamarono sull'accaduto danni non solo ai dati dei calcolatori ma addirittura all'Hardware. Nell'occasione il Ricercatore Anti-Virus Gianfranco Tonello svolse sul codice virale una dettagliata analisi tecnica e successivamente con articolo sul quotidiano economico "Il Sole 24 ORE" di Venerdì 30 settembre 1994 nell'articolo "Troppo allarmismo sul virus in edicola" chiarì il funzionamento del virus e la metodologia di propagazione dello stesso. Nell'occasione il virus, come detto, non era legato al file contenuto nel dischetto, ma si trovava nel settore di BOOT dello stesso, e la sua propagazione era legata all'eventuale utilizzo del supporto magnetico come dischetto BOOTABLE, oppure ad una sua eventuale dimenticanza all'interno del drive all'atto dell'accensione della macchina.
Nel prossimo elenco le infezioni relative allo Yankee_Doodle.Wobble non verranno più conteggiate, così da ottenere dei dati omogenei, infatti gli altri codici virali monitorati non hanno avuto la "fortuna" di essere stati diffusi grazie alla diffusione capillare di files infetti.

N°	Nome Virus	N°	%
01	Junkie.1027	173	19,79%
02	Arianna.3375	95	10,87%
03	Form	72	8,24%
04	B1	45	5,15%
05	Invisible_Man.2926	43	4,92%
06	Topa.2456	35	4,00%
07	Vota_DC.591	31	3,55%
08	November_17th.900.C	30	3,43%
09	November_17th.998	29	3,32%
10	RebelBase	27	3,09%
11	Datalock	23	2,63%
12	November_17th.800.A	21	2,40%
13	November_17th.800.B	19	2,17%
14	November_17th.900.B	18	2,06%
15	Gippo.EpidemicWare	15	1,72%
16	GoldBug	13	1,49%
17	Yeke.1204	13	1,49%
18	November_17th.855.A	12	1,37%
19	Tai-Pan	12	1,37%
20	November_17th.768	12	1,37%
21	November_17th.1007	12	1,37%
22	Jerusalem.1808.Standard	9	1,03%
23	Marzia.D	9	1,03%
Altri 26 virus		106	12,13%
TOTALE		874	100%

Virus italiani e/o virus stranieri

Come si può vedere dalla tabella riportata i virus segnalati attivi in Italia nel 1994 sono stati 50, di cui 30 sono stati creati da autori italiani (o che si "firmano" tali) mentre 20 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.

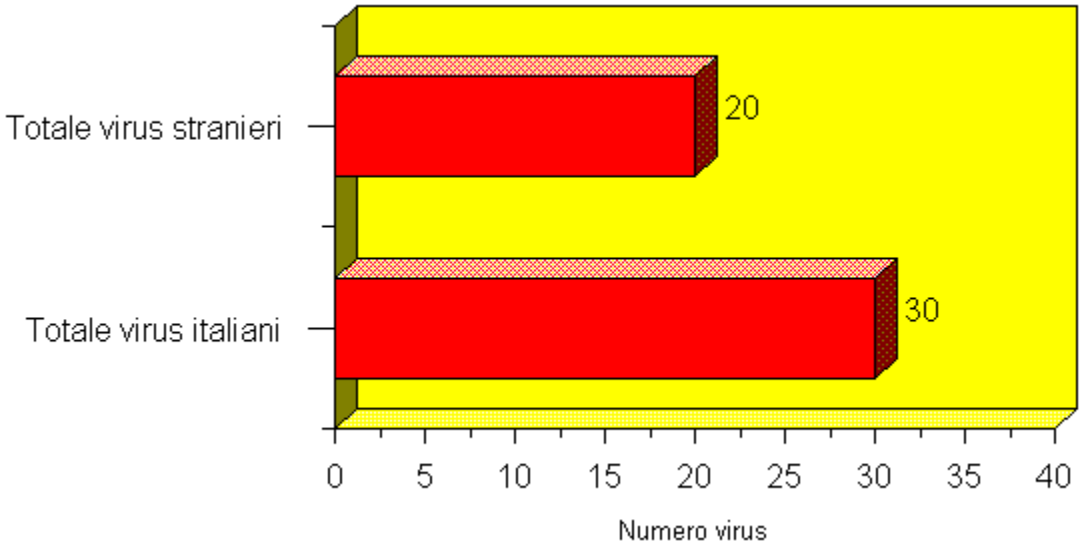
Elenco dei VIRUS prodotti presumibilmente in ITALIA

N.	Nome VIRUS	N. Inf.	%	% Cum.
01	Yankee_Dooble.Wobble	861	49,63%	49,63%
02	Arianna.3375	95	5,48%	55,10%
03	Invisible_Man.2926	43	2,48%	57,58%
04	Topa.2456	35	2,02%	59,60%
05	Vota_DC.591	31	1,79%	61,38%
06	November_17th.900.C	30	1,73%	63,11%
07	November_17th.998	29	1,67%	64,78%
08	RebelBase	27	1,56%	66,34%
09	November_17th.800.A	21	1,21%	67,55%
10	November_17th.800.B	19	1,10%	68,65%
11	November_17th.900.B	18	1,04%	
12	Gippo.EpidemicWare	15	0,87%	
13	November_17th.1007	12	0,69%	
14	November_17th.768	12	0,69%	
15	November_17th.855.A	12	0,69%	
16	Marzia.D	9	0,52%	
17	Jerusalem.1808.Standard	9	0,52%	
18	Ping_Pong	8	0,46%	
19	Gullich	6	0,35%	
20	Lubec_II.736	6	0,35%	
21	Lubec_II.1135	6	0,35%	
22	HLLC.Crawen.8306	6	0,35%	
23	StarDot.801	5	0,29%	
24	Marzia.C	5	0,29%	
25	Gippo.Stunnig_Blow	5	0,29%	
26	Polifemo.906	4	0,23%	
27	Gippo.JumpingJack	4	0,23%	
28	Marzia.B	4	0,23%	
29	HLLC.Crawen.8515	4	0,23%	
30	Italy	3	0,17%	
	Totale infezioni da virus italiani	1344	77,46%	

Elenco dei VIRUS prodotti presumibilmente all'estero

N.	Nome VIRUS	N. Inf.	%	% Cum.
01	Junkie.1027	173	9,97%	9,97%
02	Form	72	4,15%	14,12%
03	B1	45	2,59%	16,71%

04	Datalock	23	1,33%	18,04%
05	Yeke.1204	13	0,75%	18,79%
06	GoldBug	13	0,75%	19,54%
07	Tai-Pan	12	0,69%	20,23%
08	Dir_II	6	0,35%	20,58%
09	AntiExe	6	0,35%	20,92%
10	Cascade.1704	5	0,29%	21,21%
11	V-Sign	4	0,23%	
12	Parity_Boot.A	3	0,17%	
13	Keypress.1232.A	3	0,17%	
14	Ripper	3	0,17%	
15	_571	2	0,12%	
16	Michelangelo	2	0,12%	
17	Run_error_504D:5658	2	0,12%	
18	Stoned	2	0,12%	
19	Brain.Ashar	1	0,06%	
20	Yankee_Doodle.44	1	0,06%	
	Totale infezioni da virus stranieri	391	22,54%	



Dagli elenchi sopra riportate risulta che il 77,46% delle infezioni rilevate sono state prodotte da virus di origine italiana, mentre il 22,54% è stata originata da virus "stranieri". Dall'analisi dell'elenco dei codici virali stranieri, si evince, che molti di questi sono virus di "vecchia generazione" come il Michelangelo, il Form, lo Stoned etc., virus che vengono riconosciuti e in alcuni casi anche rimossi dallo stesso MSAV (anti-virus dato come 1° equipaggiamento nelle versioni DOS Microsoft a partire dalla 6.0) quindi facilmente individuabili e debellabili grazie a tale software. Per ciò che riguarda i virus italiani questi sono tutti di ultimissima generazione, non identificati da MSAV quindi difficilmente individuabili e/o debellabili con l'uso di tale software, analogo

discorso vale anche per altri anti-virus a diffusione internazionale, i quali per aggiornare i loro Dbase di FIRME virali con il materiale proveniente dall'Italia impiegano dai 6 ai 9 mesi.

I virus più resistenti

I Virus più resistenti si sono dimostrati 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 degli HardDisk operano l'infezione continua di tutti i dischetti inseriti. Non trasmettendosi attraverso i files, e quindi non allungandoli, non producono alcun segno visibile della loro azione, continuando la macchina, nella maggior parte dei casi, a funzionare in modo apparentemente corretto. Dall'elenco dei virus soprattutto stranieri si può vedere che quelli di BOOT sono rappresentati in maniera consistente, e sono soprattutto virus di vecchia generazione quali il FORM, il Ping Pong, il Michelangelo e lo Stoned. Quello che ci chiediamo è perchè questi virus, come detto identificati in molti casi anche da MSAV continuino ad essere segnalati attivi in Italia. La risposta è abbastanza semplice, questi codici virali erano all'interno di vecchi dischetti magari dimenticati sul fondo di qualche cassetto, che una volta ritrovati dai loro proprietari hanno avuto la malaugurata idea di andarne a vedere il contenuto. Quindi non si tratta in molti casi di vere e proprie infezioni di macchine, ma del loro ritrovamento all'interno di vecchi floppy.
A parte lo Yankee_Doodle.Wobble, virus che infetta i file .COM .EXE e files Overlay, troviamo nelle prime posizioni virus fast infection (infezione veloce), multipartiti quali Junkie.1027, Arianna.3375 e Invisible_Man.2926. Nelle prime 10 posizioni troviamo 5 virus che si trasmettono "solamente" attraverso i files (Yankee_Doodle.Wobble, Topa.2456, Vota_DC.591, November_17th.900.C, November_17th.998), gli altri 5 si trasmettono sia attraverso i files che attraverso il BOOT SECTOR e/o l'MBR (Junkie.1027, Arianna.3375, Invisble_Man.2926), oppure solamente attraverso il Boot Sector (Form,B1).

VIRUS INFETTANTI I "SOLI" FILES

N.	Nome Virus	N. Inf.	%
01	Topa.2456	35	4,00%
02	Vota_DC.591	31	3,55%
03	November_17th.900.C	30	3,43%
04	November_17th.998	29	3,32%
05	RebelBase	27	3,09%
06	Datalock	23	2,63%
07	November_17th.800.A	21	2,40%
08	November_17th.800.B	19	2,17%
09	November_17th.900.B	18	2,06%
10	Gippo.EpidemicWare	15	1,72%
11	Yeke.1204	13	1,49%

12	November_17th.855.A	12	1,37%
13	Tai-Pan	12	1,37%
14	November_17th.768	12	1,37%
15	November_17th.1007	12	1,37%
16	Jerusalem.1808.Standard	9	1,03%
17	HLLC.Crawen.8306	6	0,69%
18	Lubec_II.1135	6	0,69%
19	Lubec_II.736	6	0,69%
20	Dir_II	6	0,69%
21	Gippo.Stunnig_Blow	5	0,57%
22	Cascade.1704	5	0,57%
23	StarDot.801	5	0,57%
24	HLLC.Crawen.8515	4	0,46%
25	Gippo.JumpingJack	4	0,46%
26	Polifemo.906	4	0,46%
27	Keypress.1232.A	3	0,34%
28	_571	2	0,23%
29	Yankee_Doodle.44	1	0,11%
TOTALE VIRUS infettanti i files		375	42,91%

VIRUS INFETTANTI IL "SOLO" BOOT SECTOR

N.	Nome Virus	N. Inf.	%
01	Form	72	8,24%
02	B1	45	5,15%
03	Ping_Pong	8	0,92%
04	Gullich	6	0,69%
05	AntiExe	6	0,69%
06	V-Sign	4	0,46%
07	Italy	3	0,34%
08	Parity_Boot.A	3	0,34%
09	Ripper	3	0,34%
10	Michelangelo	2	0,23%
11	Run_error_504D:5658	2	0,23%
12	Stoned	2	0,23%
13	Brain.Ashar	1	0,11%
TOTALE VIRUS infettanti il Boot Sector		157	17,96%

VIRUS AD INFEZIONE MULTIPARTITA

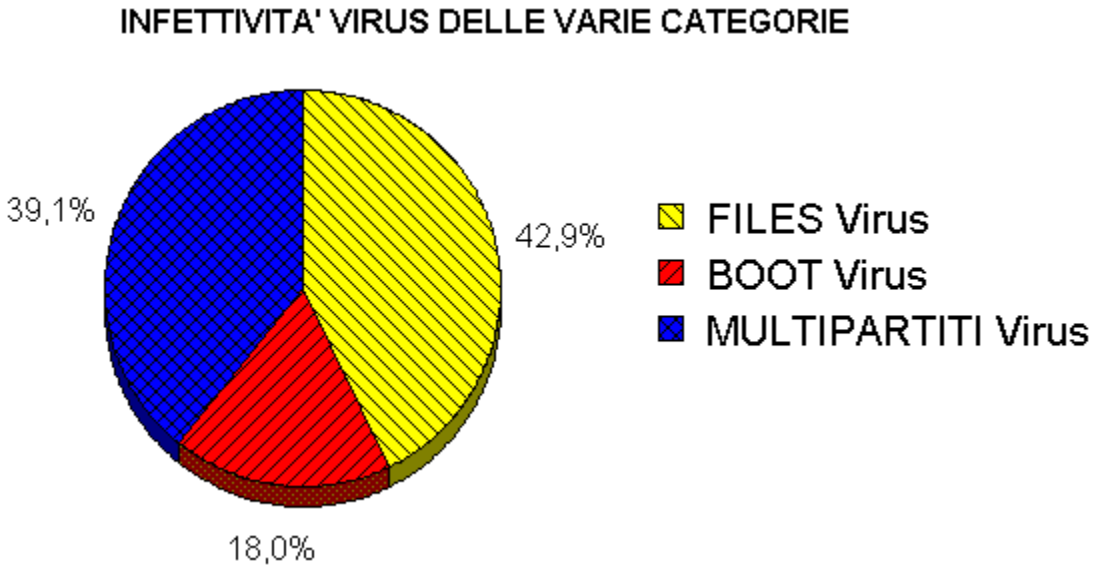
N.	Nome Virus	N. Inf.	%
01	Junkie.1027	173	19,79%
02	Arianna.3375	95	10,87%
03	Invisible_Man.2926	43	4,92%
04	GoldBug	13	1,49%
05	Marzia.D	9	1,03%
06	Marzia.C	5	0,57%
07	Marzia.B	4	0,46%
TOTALE Virus ad infezione multipartita		342	39,13%

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. E' 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.

Accorpamento dei dati di infettività per categoria

N.	CATEGORIA VIRUS	N. Inf.	%
29	FILES Virus	375	42,91%
13	BOOT Virus	157	17,96%
7	MULTIPARTITI Virus	342	39,13%
49	TOTALE	874	100%



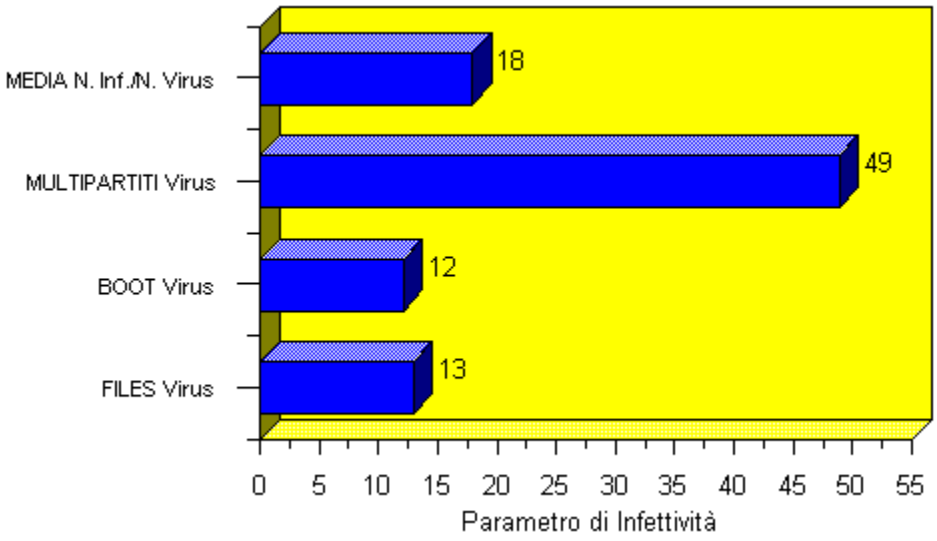
INFETTIVITA' DEI VIRUS DELLE VARIE CATEGORIE

Si è cercato un parametro che esprimesse l'infettività delle varie categorie di virus, infettività intesa come maggiore o minore capacità di una certa categoria di virus a diffondersi, cioè ad infettare computer (cioè a propagarsi).
Il parametro è stato individuato nel semplice rapporto tra il numero di infezioni monitorate per categoria ed il numero di virus distinti che le hanno provocate e verra indicato con il simbolo P.I.

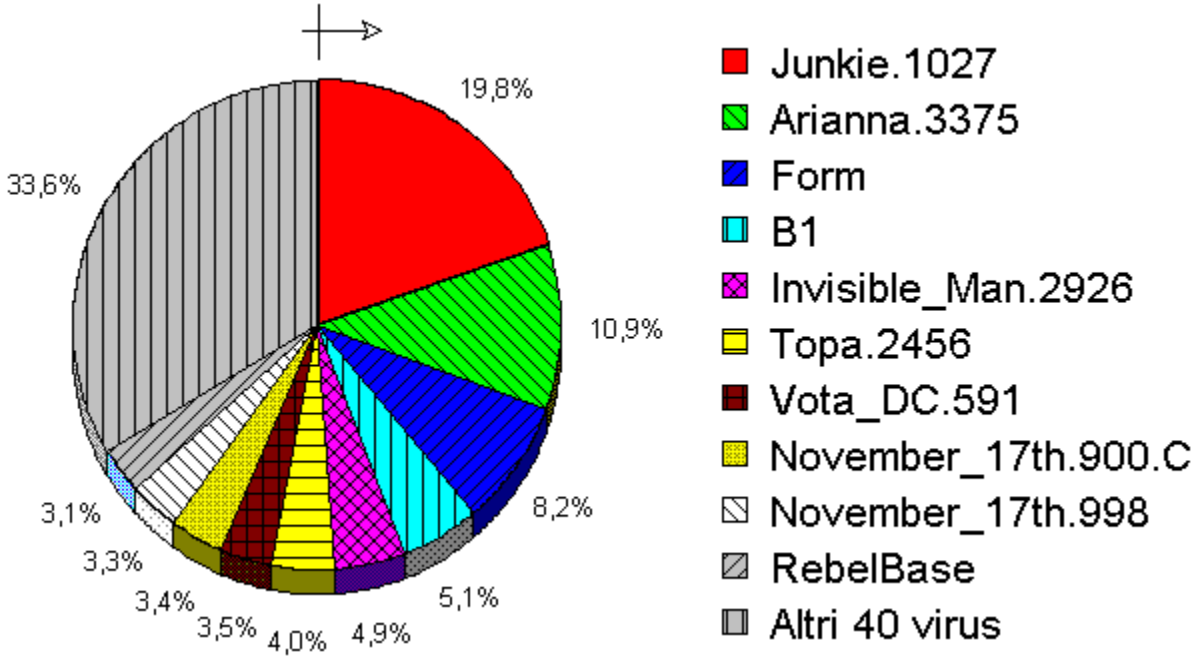
N.	CATEGORIE VIRUS	N. Inf.	P.I.
29	FILES Virus	375	12,93
13	BOOT Virus	157	12,08
7	MULTIPARTITI Virus	342	48,86

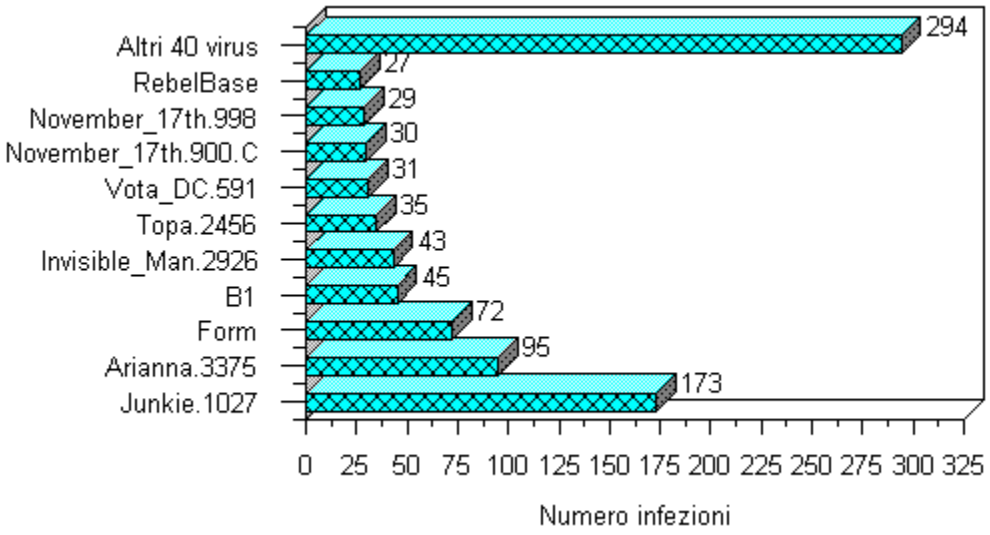
49	MEDIA N. Inf./N. Virus	874	17,84

Come si può vedere i Virus MULTIPARTITI sono risultati i più infettivi (oltre 3 volte più infettivi) rispetto ai Virus delle altre due categorie. Questo è uno dei risultati che era lecito attendersi tenuto conto che questi uniscono le peculiarità di ambedue le categorie di virus.



Top Ten Virus





Conclusioni

Da quanto esposto risulta chiaro che i Virus MULTIPARTITI sono quelli che hanno maggiore diffusione, sebbene siano ancora in numero limitato, se i virus-writers continueranno a produrli, e questa sembra essere la tendenza, potrebbero arrivare a produrre danni anche ingenti su scala nazionale ed anche oltre. I virus-writers "italiani", o considerati tali, sono maggiormente "portati" alla produzione di FILES VIRUS, ma nel 1994 si è notato che l'interesse di alcuni si è spostata verso i Virus MULTIPARTITI. Infatti dei 7 Virus MULTIPARTITI circolanti in Italia, ben 5 possono essere imputati ad autori italiani (Arianna.3375, Invisible_Man.2926, Marzia.D, Marzia.C e Marzia.B). Alla comunità informatica italiana e mondiale non resta che sperare che questi fantomatici personaggi si ravvedano e spostino il loro interesse verso programmi di maggiore utilità sociale. Per quanto ci riguarda, non ci resta, che essere attenti all'osservazione del fenomeno VIRUS, confidando soprattutto nella collaborazione dell'intera comunità informatica, la quale ad ogni ritrovamento di codice virale dovrebbe operare la sua segnalazione ed eventualmente l'invio di campioni per l'analisi, permettendo ai ricercatori anti-virus di mettere a punto apposite contromisure per combatterli.

COME SI SEGNALANO LE INFEZIONI IN ATTO

VirIT -Il Servizio Anti-Virus italiano- già da 2 anni si occupa di monitorare il fenomeno a livello nazionale, andando a raccogliere in modo certosino le infezioni in atto nel territorio nazionale. I dati monitorati sono:

Nome Virus _____ Rilevato con _____

Computer infetti N° _____ il __/__/__ Provincia _____

[ ] AZIENDA [ ] PRIVATO

Questi dati possono essere comunicati a mezzo telefono 049-631748 (TG Soft - Il Servizio Anti-Virus italiano-) oppure inviati per via telematica ai seguenti indirizzi:
FIDO NET: Gianfranco Tonello 2:333/316.4
INTERNET: tge@maya.dei.unipd.it

Analisi di alcuni virus tra i più diffusi

coordinatore Gianfranco Tonello

- Satyricon
- Bloody_Warrior
- Maaike
- HDKiller

Satyricon

Nome virus:	Satyricon
Aliases:	
Variante:	184
Isolato:	Settembre 1993
Sintomi:	lunghezza dei files aumentata
Origine:	Italia (?)
Dimensione:	360 bytes
Tipo:	Azione diretta, infetta .COM
Analisi a cura di:	Gianfranco Tonello
Rimozione:	VirIT

Commento generale:

Questo codice virale è stato individuato nella seconda settimana di settembre 1993, la sua provenienza è quasi sicuramente italiana. Il virus è ad azione diretta ed infetta i files .COM della corrente directory.
Quando un programma infetto dal Satyricon viene eseguito, il virus legge la data del sistema, se corrisponde al giorno 13 si inluppa, altrimenti infettera' tutti i file con estensione .COM nella corrente directory con il penultimo byte diverso da 0AFH. Dopo di che infetterà il file FORMAT.COM presente nella directory C:\DOS.
La lunghezza dei files aumenterà dai 360 ai 375 bytes, questa variazione è dovuta all'allineamento di paragrofo eseguito dal codice virale prima dell'infezione, data e ora dei files colpiti non vengono modificate.
All'interno del codice sono presenti le seguenti stringhe:

" *.COM "

" C:\DOS\FORMAT.COM "

" SATYRICON "

Quest'ultima stringa non viene mai visualizzata a video.
Il virus oltre alla sua propagazione con le modalità già viste non risulta procurare danni di sorta, si può facilmente desumere dalla "qualità" e "funzionalità" del codice, che questo non può che essere un virus di sperimentazione.

Bloody_Warrior

Nome virus:	Bloody_Warrior
Aliases:	
Variante:	
Isolato:	10 Dicembre 1993
Sintomi:	lunghezza dei files .EXE e .COM aumentata, diminuzione della memoria libera del sistema
Origine:	Italia
Dimensione:	1344 bytes
Tipo:	Residente in memoria, crittografato, infetta .EXE e .COM
Analisi a cura di:	Gianfranco Tonello Tel. 049/631748
Rimozione:	VirIT by Gianfranco Tonello

Commento generale:

Questo codice virale è stato individuato nella prima settimana di dicembre 1993, la sua provenienza è sicuramente italiana. Il virus è residente in memoria (TSR), crittografato ed infetta i file con estensione .EXE e .COM.
Quando un programma infetto dal Bloody_Warrior viene eseguito il virus si installa in memoria allocando 2768 bytes ed intercetta gli interrupts 21H (funzioni DOS) e 24H (gestione degli errori critici).
Ogni file eseguito, aperto, rinominato, letto o modificato negli attributi, con estensione .EXE e .COM (con lunghezza infeziore a 60.000 bytes) verrà infettato, la lunghezza dei file colpiti aumenterà di 1344 bytes.
Il virus prima di procedere all'infezione del file ne controlla il nome, verifica se la parte terminale del nome dei files .COM finisce con:

"STOP" (corrispondente al VIRSTOP.COM di F-Prot),

invece per i file .EXE se termina con:

"SCAN" (SCAN.EXE di McAfee Associates),
"SHIELD" (VSHIELD.EXE di McAfee Associates),
"CLEAN" (CLEAN.EXE di McAfee Associates),
"CV" (CODEVIEW.EXE Microsoft),
"DEBUG" (DEBUG.EXE del DOS) e
"TD" (TD.EXE Turbo Debugger Borland),

allora si disattiva dalla memoria, cioè risetta l'interrupts 21H con i vettori

originali (quelli relativi a prima che si installasse in memoria).
I file .COM infetti saranno marcati all'offset 6 con la WORD 7347H, mentre i file .EXE saranno marcati all'offset 12H. Data e ora dei file infetti non vengono alterate. Il virus si attiva tutti i giorni a partire dal 4 luglio fino alla fine del mese, sovrascrivendo 256 settori partendo dal settore logico nø 1 del disco corrente con valori casuali.
All'interno del codice virale, dopo la sua decrittografazione, sono visibili le seguenti stringhe, le quali non vengono mai visualizzate a video:

" FUCK YOU "
" EXECOMSCANSTOPSHIELDCLEANCVDEBUGTD "
" Hello, world ! I am the Bloody Warrior. Nice to meet you. "
" What about this virus ? Funny ? There is no hope for you. "
" This virus was released in Milan 1993. Bloody Warrior "

Maaike

Nome virus:	Maaike
Aliases:	250
Variante:	
Isolato:	Maggio 1994
Sintomi:	diminuzione della memoria libera del sistema, files .COM nascosti, messaggio a video;
Origine:	Sconosciuta
Dimensione:	250 bytes
Tipo:	Residente, gemellare, polimorfico, crittografato,stealth, infetta .EXE creando un file .COM nascosto;
Analisi di:	Gianfranco Tonello Tel. 049-631748
Rimozione:	VirIT

Commento generale:

Questo codice virale è stato individuato nella seconda settimana di maggio 1994, la sua provenienza non è conosciuta. Il virus è residente in memoria, polimorfico, stealth, infetta .EXE creando un file con lo stesso nome, ma con estensione .COM e con attributo nascosto (H=hidden). La lunghezza del file .COM (contenente il VIRUS) è di 250 bytes.
Quando si esegue un programma con estensione .EXE, se nella directory è presente un file con identico nome ma con estensione .COM, il DOS manda in esecuzione quest'ultimo. In questo modo viene eseguito il Virus Maaike, il quale si installerà in memoria allocando 507 bytes ed intercettando l'interrupt 21H del Dos.
Dopo l'allocazione in memoria, ogni file eseguito, anche con estensione .COM, sarà modificato nell'estensione, che verra' tramutata in .EXE, e successivamente eseguito.
Questa tecnica, oltre a permettere l'esecuzione del vero e proprio programma, consente di implementare una particolare tecnica stealth. Infatti cercando di debuggare un file virato con il programma DEBUG, ad esempio DEBUG PIPPO.COM,
il Virus modifica l'estensione del file in .EXE eseguendo il comando DEBUG PIPPO.EXE che visualizzerà il programma e non il codice virale.
Dopo l'esecuzione del programma, il virus Maaike preleva un valore casuale dal system clock interrupt (irq 0/int 08), confronta la parte bassa di tale valore con 0EH, se si verifica l'uguaglianza, viene scritto nella pagina testo B800H il seguente testo lampeggiante:

" Maaike I Love You ! "

in verde su sfondo rosso per un totale di 105 volte. Altrimenti il codice si crittografa e viene creato un file di 250 bytes con il nome del programma eseguito precedentemente, ma con estensione .COM e con attributo nascosto. Il Virus Maaike risulta essere anche polimorfico, polimorfismo ottenuto invertendo solamente l'ordine dei registri, il metodo di crittografazione rimane invariato.

HDKiller

Nome virus:	HDKiller
Aliases:	La Coruna 4
Isolato:	Roma, Marzo 1995
Sintomi:	Diminuzione memoria libera del sistema
Origine:	Sconosciuta
Dimensione:	512 bytes
Tipo:	Infetta boot sector e Master boot record
Analisi a cura di:	Gianfranco Tonello
Rilevazione:	VirIT

Commento generale:

Virus residente in memoria, infetta boot sector dei floppy disk e master boot record (mbr) dell'hard disk. Quando viene eseguito il boot da un floppy infetto da HDKiller, il codice virale infetta il master boot record dell'hard disk e viene eseguito il boot da disco fisso. Il codice virale si è installato in memoria occupando 1 Kb, ed intercettando l'interrupt 13H e 1CH, successivamente ogni floppy disk verrà infettato. Il codice virale non preserva il boot e master boot record precedenti, per questo motivo il clean non è realizzabile venendo a mancare i dati originali.
Il virus scrive nella tavola delle partizioni il giorno che ha infettato il PC decrementato di uno. Il valore del giorno viene restituito dal sistema in formato BCD (Binary Decimal Code), quando viene decrementato dal virus, questo valore può perdere riferimento nel formato BCD, il quale utilizza solo le prime 10 cifre del binario puro ed assegnandole alle corrispondenti decimali. Quando il codice virale parte da master boot record, esegue la comparazione del giorno (BCD) con quello decrementato, se sono uguali allora viene sovrascritto il disco fisso. All'interno del codice è presenta la seguente stringa:

HDKiller By Rasek.0UT Meilàn!

INSANE REALITY

di Gianfranco Tonello

E' stato ritrovato il #4 numero della rivista ipertestuale INSANE REALITY redatta dal fantomatico gruppo di Virus Writers IMMORTAL RIOT (di origine svedese).
L'ipertesto è caratterizzato da una struttura DESK TOP, costituita da 5 menù a tendina (come si può vedere dall'immagine sotto).

INFORMATION

all'interno di questo sottomenù vi sono i membri dell'organizzazione. I particolari ringraziamenti a coloro che hanno contribuito con il loro materiale alla realizzazione "dell'opera". Vengono citati tra gli altri anche produttori & studiosi anti-virus di fama internazionale quali: FRISK INT, TBAV, S&S INTERNATIONAL, DATA FELLOWS e VSUM. Questi studiosi vengono ironicamente citati, in

relazione al loro lavoro contro la diffusione dei codici virali.

ARTICLES

All'interno vi sono 10 articoli:

01) vengono innanzitutto presentate le novita' presenti in questo numero della rivista ipertestuale, rispetto alla precedente;

02) viene operata una cronistoria dettagliata degli avvenimenti accaduti tra l'uscita del #3 e #4 numero della rivista;

03) modalità per "rintracciare" gli autori della rivista! Su alcuni vi sono i numeri telefonici, su altri, vi è solamente il prefisso del distretto. Ipotizzando che tali numeri siano "veri" si potrebbe risalire alla dislocazione spaziale dei redattori;

04) descrizione dei numeri precedenti;

05) articolo sul report del Bollettino 2.11 della DATA FELLOWS che cita il gruppo degli IMMORTAL RIOT (un po' di auto celebrazione);

06) la "vera" storia del VCL Olimpic, in contropposizione con le notizie apparse sul Bollettino 2.11 Data Fellows;

07) commento sulle informazioni riportate dagli anti-virus. Report degli errori commessi da Mikko Hypponen (Data Fellows) sull'analisi dei vari "prodotti" degli IMMORTAL RIOT;

08) articolo dedicato al VSUM by Patricia Hoffman, la quale viene ironicamente derisa dai VW (Virus Writers), tanto da arrivare a prenderla in giro con telefonate "anonime". Commento su due analisi virali relative al My Little Pony e al DNR virus;

09) informazioni generiche sui virus;

10) i piani futuri degli IMMORTAL RIOT.

INTERVIEWS

All'interno vi sono 9 interviste ad alcuni "famosi" Virus Writers.
Interessante è l'articolo su "PERSONA NO GRATA", nel quale viene infatti ringraziato DOCTOR REVENGE (autore dell'omonimo virus Doctor_Revenge.1979, Dream_Man e Peace Keeper), identificato come rappresentante per l'Italia dell'organizzazione NUKE (organizzazione già autrice del VCL).

VIRUSES

All'interno vi sono 9 diversi sorgenti di codici virali commentati dagli stessi autori. Mi preme sottolineare l'aspetto "educativo" del tutto. Infatti i sorgenti commentati, sono indiscutibilmente, uno dei mezzi per l'alfabetizzazione dei "nuovi" scrittori di virus. I sorgenti sono anche disponibile all'interno di un file .ZIP sfusi, pronti per essere compilati, e quindi per dar vita (se diffusi) ad epidemie.

VGA-Art

All'interno vi sono 7 immagini del Logo degli IMMORTAL RIOT (anche l'occhio vuole la sua parte....).

Collabora con Italian VIRUS Magazine

Sei un ricercatore Anti-Virus, sei in grado di analizzare un codice virale, hai notizie o informazioni riguardanti i virus informatici MS-DOS, che abbiano qualche interesse per la comunità informatica italiana?
Contatta la redazione di Italian VIRUS Magazine scrivi a:

TG Soft
Via Sardegna n° 5
35030 Sarmeola di Rubano (PD)

Allega una tua presentazione e/o un tuo curriculum, nonchè una traccia del materiale in tuo possesso. Se tale materiale sarà ritenuto interessante per la pubblicazione sarai ricontattato ed invitato a scrivere un articolo.

Index

Glossary

≡
#
A
B
C
D
E
F
G
H
I
J
K
L
M
N
O
P
Q
R
S
T
U
V
W
X
Y
Z

C

Cavallo di troia

CODICI VIRALI

E

EURISTICO

F

FIRME VIRALI

T

TG Soft

TROJAN

V

virus

Cavallo di troia

Trojan horse, o cavallo di troia:Programma che nasconde sotto una facciata innocua ed invitante un programma killer che generalmente distrugge i dati dell'hard disk

CODICI VIRALI

Sinonimo di virus informatico, ossia il vero e proprio programma che é in grado di autoreplicarsi.

EURISTICO

Metodo che consente di determinare se un programma esegue operazioni sospette, ossia operazioni tipiche dei virus informatici permette pertanto di intercettare dei virus di cui non si conosce ancora la firma virale.

FIRME VIRALI

Il codice esadecidemale che permette di identificare il virus. I virus polimorfici cercano di automodificarsi per non farsi intercettare dai comuni antivirus.

TG Soft

Software house specializzata in Sicurezza Informatica con particolare attenzione nel campo della lotta anti-virale in ambiente MS-DOS. Tel. 049/631748

TROJAN

Trojan horse, o cavallo di troia:Programma che nasconde sotto una facciata innocua ed invitante un programma killer che generalmente distrugge i dati dell'hard disk

virus
Programma in grado di autoreplicarsi.