# YEKE e le sue varianti

di Gianfranco Tonello

Nel 1993 e nella prima metà del 1994 si è registrato un notevole incremento di virus italiani, mentre nel biennio 1991-92 i codici virali di sicura produzione italiana erano da un punto di vista numerico estremamente esigui, non oltre la decina, prodotti per lo più dall'estro goliardico di qualche "ingegnoso" studente.

Queste creazioni, nella maggior parte dei casi, non sono state utilizzate per la generazione di infezioni di elevate dimensioni (tranne nel caso dell'ormai vetusto Ping-Pong e del più recente November_17th.855), ma al solo scopo di provare, da parte dell'autore, le proprie capacità tecniche. La proliferazione dei virus citati fu legata alla novità assoluta del fenomeno ed alla inevitabile mancanza di contromisure preventive.

Ora però il fenomeno ha avuto un sensibile incremento sia da un punto di vista numerico, sia da un punto di vista tecnico. Si sono notati notevoli progressi, che hanno portato gli scrittori di virus di casa nostra quasi ai livelli dei più famosi autori stranieri, quali: il bulgaro Dark Avenger, il nord americano Nowhere Man e lo svizzero Psycoblast (autore di svariate varianti del virus Flip).

Si è passati dai primi codici virali che si limitavano a replicarsi e a dare vita di tanto in tanto a performance video anche godibili quali il Ping-Pong e l'Itavir a creazioni molto più sofisticate, in grado di rendersi invisibili (utilizzando tecniche stealth), e/o bypassare gli ormai diffusissimi software di monitoraggio TSR ricercando i vettori originali degli interrupt (tecniche di tunneling). Uno tra i prodotti testimonial di questa nuova generazione di codici virali, basato su "tecnologie" Flip, risulta essere l'Invisible_Man (creazione di un anonimo salernitano innamorato).

Se all'inizio i virus venivano camuffati con tecniche di crittografazione a chiave fissa o al più a chiave variabile, in quest'ultimo biennio le routine atte allo scopo si sono notevolmente affinate. Si è passati dalla crittografia al polimorfismo, ciò è stato possibile grazie all'abilità tecnica dei singoli autori (come nel caso dell'Invisible_Man), ma soprattutto grazie alla comparsa dei vari motori polimorfici: MtE (Mutation Engine), TPE (Trident Polymorphic Engine) e altri meno noti al grande pubblico.

Questi motori permettono di assemblare ad un qualsiasi virus una routine che lo crittografi in modo multivariato, rendendo così ogni replicazione diversa dalla precedente, anche in lunghezza.

Nei primi tempi gli scrittori di virus erano per la maggior parte dei solitari – seppur a volte nascosti dietro sigle "plurali", quali l'I.V.R.L. (Italian Virus Research Laboratory) – depositari delle conoscenze più profonde sui pregi e sui difetti del sistema operativo MS-DOS.

Successivamente si è notato un inizio di associazionismo tra scrittori di virus, basti pensare alla recente scoperta del fantomatico ELECTRONIC SHEEPSTEAM che ha prodotto virus come il Trickster ed il TPE Lamers Exterminator. Oltre a questi è comparso recentissimamente un nuovo gruppo di virus-writer che si firma con la sigla IVL (Italian Virus Lab) e che ha già prodotto oltre una decina di codici virali attraverso l'uso di un generatore di virus chiamato IVP.

Sono proprio i generatori di virus, sebbene i codici virali generati siano, almeno per ora, non eccelsi da un punto di vista prettamente tecnico, che possono mettere in condizione anche persone dalle limitate conoscenze nel campo della programmazione Assembly di realizzare in pochi minuti nuovi codici virali, che non essendo identificati dagli scanner più diffusi, potranno originare infezioni incontrollate.

Altro esempio eclatante di software generativo, forse più famoso e diffuso del precedente, è rappresentato dal VCL, il quale, pur non producendo codici virali dalle eccelse qualità, dà però la possibilità ad un comune utente di poter vestire in pochi minuti i panni del virus-writer. Questa possibilità è legata alla sua "facilità d'uso", che

permette di creare un codice virale con le caratteristiche desiderate.

E' proprio da questa evoluzione che nasce l'esigenza di creare una rubrica periodica di informazione e news sul mondo dei virus, con particolare attenzione ai codici circolanti e/o di creazione italiana.

Inizieremo quindi la nostra analisi tecnico-evolutiva con la descrizione di due codici virali scoperti all'inizio del 1993, due varianti del virus YEKE.

### YEKE.1204

*Alias:* BOAT, ReFReF, 1204

*Isolato:* Gennaio 1993

*Sintomi:* Lunghezza dei file .EXE aumentata; diminuzione della memoria libera del sistema; modalità grafica CGA 40x25, sottofondo musicale

*Origine:* Sconosciuta

*Dimensione:* 1204 bytes

*Tipo:* Residende in memoria (TSR), crittografato, infetta .EXE

*Identificazione:* Scan 99+, VirIT 0.93+

*Rimozione:* Scan 111+, VirIT 0.93+

## Commento generale

Il virus YEKE.1204 è stato isolato in Italia nel mese di gennaio 1993, la provenienza è però sconosciuta. Le prime segnalazioni vengono dalla regione Lombardia presso il Politecnico di Milano.

Questo virus è residente in memoria, infetta i files .EXE ed è a crittografazione variabile. Quando un programma infetto dallo YEKE.1204 viene eseguito il virus si installa nella parte alta della memoria dei 640 Kbytes allocando 2.496 bytes, ed intercettando l'interrupt 21H (funzioni DOS) e 24H (gestione degli errori). Dopo l'installazione in memoria ogni programma .EXE eseguito, di lunghezza compresa tra 10.000 e 327.679 byte viene infettato, se questo risulta essere già infetto il virus lo disinfetta e lo manda in esecuzione, all'uscita del programma il virus lo reinfetta.

Il file infetto aumenta di 1204 bytes, data e ora non vengono alterate. Lo YEKE.1204 contiene al suo interno la seguente stringa crittografata:

```
ReFReF TReF
```

Il Virus rende visibili i suoi effetti il 23 marzo di ogni anno, dopo 30 minuti dalla sua attivazione, visualizzando a video in modalità grafica CGA 40x25 la seguente stringa:

```
Be Careful. YEKE
controls Your Computer
```

con sottofondo musicale.

### YEKE.1076

*Variante:* YEKE.1204

*Isolato:* Marzo 1993

*Sintomi:* Lunghezza dei file .EXE aumentata; diminuzione della memoria libera del sistema; modalità grafica CGA 40x25, sottofondo musicale

*Origine:* Sconosciuta

*Dimensione:* 1076 bytes

*Tipo:* Residende in memoria (TSR), crittografato, infetta .EXE

*Identificazione:* Scan 99+, VirIT 0.93+

*Rimozione:* VirIT 0.93+

## Commento generale:

Il virus YEKE.1076 è stato isolato in Italia nel mese di marzo


1993, la provenienza è però sconosciuta.

Questo virus è residente in memoria, infetta i file .EXE ed è a crittografazione variabile. Quando un programma infetto dallo YEKE.1076 viene eseguito il virus si installa nella parte alta della memoria dei 640 Kbyte allocando 2.240 bytes, ed intercettando l'interrupt 21H (funzioni DOS) e 24H (gestione degli errori).

Dopo che lo YEKE.1076 è residente, ogni programma .EXE eseguito, di lunghezza compresa tra 20.000 e 327.679 byte viene infettato, se è infetto il virus lo "disinfetta" e viene mandato in esecuzione, al termine dell'esecuzione del programma il virus lo infetta. Il file infetto aumenta di 1076 bytes, data e ora non vengono alterate. Rispetto allo YEKE.1204 non è contenuta alcuna stringa visibile.

Il virus rende visibili i suoi effetti il 23 marzo di ogni anno, dopo 30 minuti dalla sua attivazione, visualizzando a video in modalità grafica CGA 40x25 la seguente stringa:

```
Be Careful. YEKE
controls Your Computer
```

con sottofondo musicale.

---

*Gianfranco Tonello è ricercatore antivirus, nonché autore del software di scansione e rimozione VirIT.*