# Guardie e ladri

di Stefano Toria

*Diamo uno sguardo stavolta agli... ultimi ritrovati della tecnica, sia dal lato di chi sviluppa software antivirus, sia di chi invece si dedica alla costruzione di nuovi, più sofisticati programmi aggressori*

## L'eterno conflitto

Ormai ci siamo rassegnati. Quasi ogni mese esce una nuova versione di un prodotto antivirus (attualmente ne utilizziamo tre diversi, qui in redazione), e nelle note di accompagnamento c'è la lista dei nuovi virus, che regolarmente contiene qualche sorpresa. Un paio di mesi fa si trattò dei virus a crittografia variabile; stavolta c'è addirittura un kit di sviluppo di virus. Ma procediamo con ordine.

## La fabbrica bulgara

Chi segue MC con attenzione forse rammenterà un riquadro che fu pubblicato sul n. 99, nel settembre 1990, in cui si parlava della diffusione mondiale degli sviluppatori di virus e del fatto singolare che un numero apparentemente enorme di questi programmi sembrava originare da un Paese relativamente piccolo come la Bulgaria, all'epoca ancora appartenente al blocco sovietico e quindi presumibilmente fuori del «giro» della tecnologia avanzata.

La posta elettronica non ha frontiere, abbiamo imparato già da tempo questo concetto fondamentale che in questo caso ha trovato una conferma. Inoltre la particolare situazione sociopolitica ed economica della Bulgaria, spiegavamo nell'articolo, aveva favorito la diffusione dell'attività di sviluppo di virus da parte di programmatori tecnicamente molto abili, ma impossibilitati a vendere sul libero mercato i frutti di questa loro abilità; da ciò derivava una frustrazione che in alcuni casi costituì la motivazione sufficiente per mettersi a scrivere programmi clandestini. In altre parole: se non riesco a far vedere al mondo che bravo programmatore che sono (e a far soldi) producendo fogli elettronici, programmi di comunicazione o di grafica, allora mi metto a fare virus; soldi forse non ne farò (ma non è detto e tra poco lo vedremo) ma almeno ti faccio vedere quanto sono bravo, e oltretutto colgo due piccioni con una fava: poiché i computer in Bulgaria abbondano e sono proprietà pubblica, sviluppare virus diventa anche una forma di boicottaggio politico.

Così era la situazione nel 1990 quando scrivevamo l'articolo citato più sopra. E così è tuttora in parte la situazione, pur dopo gli inevitabili sconvolgimenti dovuti alla disgregazione dell'Unione Sovietica e alle sue conseguenze. In ogni caso l'attività dei fabbricanti di virus in Bulgaria ferve ora più che mai. Il famoso «Dark Avenger», il «Vendicatore Oscuro» autore dell'omonimo virus, si è rifatto vivo ultimamente. Nessuno è ancora riuscito a rivelarne l'identità, non si sa neppure se si tratta di un singolo individuo oppure se è un gruppo di programmatori ad agire sotto questa sigla; ma l'ultimo prodotto del «Dark Avenger» dimostra ancora una volta che si tratta comunque di una persona (o di un gruppo) estremamente abile, con una profonda conoscenza del DOS e con capacità di programmazione non comuni.

## Il «Mutation Engine»

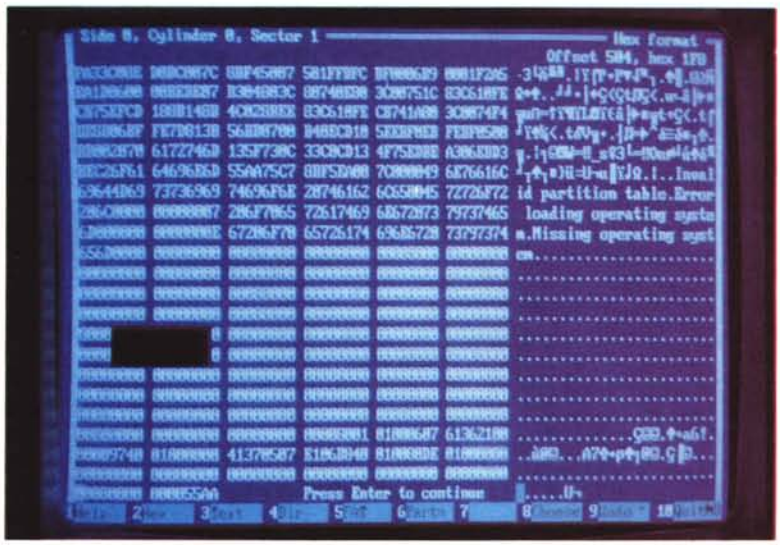
Le prime notizie su questo nuovo prodotto giungono personalmente da John McAfee. Con un messaggio spedito il 12 marzo in una conferenza elettronica sui virus, l'esperto californiano segnala la presenza di tre nuovi virus generati servendosi di un «Dark Avenger Mutation Engine».

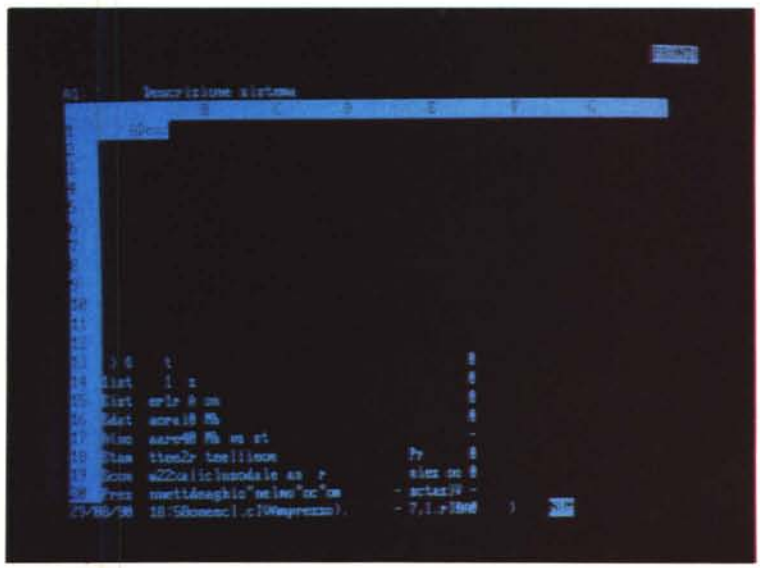
Si tratta di un notevole passo avanti nella tecnologia dei virus, che dà motivo di temere che si stia aprendo un nuovo capitolo in questa fastidiosa storia. È il primo esempio di applicazione di tecniche avanzate di programmazione allo sviluppo dei virus.

Chiunque realizza software a livelli professionali sa bene che è difficile gestire progetti di una certa dimensione senza servirsi di strumenti di sviluppo sofisticati. Editor, compilatore e debugger sono affiancati da librerie di funzioni predefinite e sistemi di descrizione di applicazioni che consentono di aumentare la produttività del programmatore e al tempo stesso di ottimizzare l'efficienza del codice generato.

Il Mutation Engine, o MtE, appartiene a questa categoria di programmi. Il numero di nuovi virus continua a crescere, la maggior parte delle novità consiste in varianti di virus arcinoti (anche questo mese sono arrivati dei nuovi Cascade, dei nuovi Jerusalem) ma ci sono anche dei virus sviluppati *ex novo*. Molti sono banali, facili da identificare; quelli che pongono seri problemi ai ricercatori sono come al solito quei virus che impiegano delle tecniche di depistaggio per nascondere la propria presenza, per rendersi invisibili e ingannare i programmi antivirus. È un gioco di guardie e ladri: qualcuno inventa un nuovo dispositivo di copertura, i programmi antivirus vengono opportunamente modificati per tenerne conto, poi qualcun altro inventa un nuovo trucco e così avanti. Il fine rimane comunque lo stesso: chi scrive virus cerca di realizzare programmi che riescano a diffondersi il più possibile senza essere identificati dai programmi di scansione, chi scrive antivirus cerca di mettere il proprio prodotto in condizione di scoprire quanto più precocemente possibile le tracce di un'infezione.

A questo proposito apriamo una parentesi per rammentare ancora una volta che i programmi antivirus, pur non costituendo una misura pienamente efficace di per sé, debbono essere mantenuti costantemente aggiornati. Ci telefonano in redazione dei lettori che affermano di servirsi di versioni che risalgono addirittura a un anno fa: tanto vale non farne uso, perché l'esperienza ha dimostrato (e i ricercatori hanno confermato) che non si può sapere in anticipo quali virus avranno ampia diffusione e quali no, e il «problema del momento» di dopodomani potrebbe essere ancora



*Il «Jerusalem» ed il Cascade rimangono tra i più diffusi virus, anche per il numero di nuove varianti che se ne riscontrano regolarmente.*

del tutto sconosciuto oggi; tanto per fare un esempio, nel marzo 1991 nessun antivirus riconosceva il «Michelangelo», che è poi risultato diffusissimo, e pertanto chi si fosse affidato a un antivirus vecchio di un anno sarebbe senz'altro rimasto vittima di questo banale programma.

Una delle tecniche di depistaggio consiste nel crittografare il corpo del virus prima di accodarlo al file da infettare. Per la crittografia ci si serve di una chiave pseudocasuale, che verrà incorporata nello stesso file bersaglio; il programma crittografato dovrà essere accompagnato da una funzione di decrittazione che verrà eseguita per prima, in modo da sottoporre al microprocessore le istruzioni decifrate: diversamente non sarebbe in grado di eseguirle. La chiave pseudocasuale assicura che non ci siano due replicazioni del virus che diano luogo a un risultato identico; in questo modo la determinazione di una «firma» del virus è più difficile perché la parte che rimane identica è limitata ai pochi byte della funzione di decrittazione. Tuttavia quest'ultima è passibile di identificazione da parte di un programma di scansione; in effetti è questo il metodo utilizzato per identificare i virus crittografati.

Per ingannare i programmi di scansione, ed evitare che i propri prodotti venissero scoperti, alcuni creatori di virus hanno pensato di far mutare casualmente la porzione di virus da registrare non crittografata. Pur mantenendo invariata la sequenza di operazioni, laddove possibile le istruzioni vengono modificate, ne vengono aggiunte di fittizie o superflue in modo tale da non consentire mai l'identificazione di una sequenza minima di byte identici tra una replicazione e l'altra. La mutazione infatti avviene ogni volta che il virus si trasmette, in modo da ottenere tanti oggetti diversi che non si somigliano neppure di poco.

Realizzare un sistema di mutazione non è cosa semplice. «Dark Avenger» è venuto incontro a chi volesse generare un virus di questo tipo, realizzando una libreria di funzioni (il MtE, appunto), che può essere incorporata in un programma in fase di link edit, portando la realizzazione di un virus mutante alla portata anche di chi non abbia le capacità sufficienti a costruirselo da sé.

È un fatto piuttosto grave di per sé, ma l'ignoto bulgaro non si è fermato qui. Sono state riportate delle voci secondo cui «Dark Avenger» avrebbe offerto di vendere i simbolici del MtE al prezzo di cinquemila dollari, da versare a un intermediario. Se fosse vero si tratterebbe del primo caso conosciuto di un virus che rende qualcosa al suo autore.

## *L'evoluzione dei sistemi antivirus*

Anche sul fronte delle «guardie» questo mese risultano alcune novità. Sul numero di febbraio abbiamo pubblicato un'intervista con McAfee, nella quale l'autore di «SCAN» esprimeva l'opinione secondo cui i programmi di scansione antivirus avrebbero continuato a rendere un servizio efficiente ancora per

molti anni. In realtà questi programmi stanno mostrando i propri limiti, ed è possibile che i prossimi mesi facciano registrare qualche clamorosa uscita dal mercato, una volta ritenuto facile e redditizio, dei programmi antivirus. L'uscita del MtE potrebbe costituire proprio l'ultima goccia per alcuni produttori di software, in special modo quelli che hanno afferrato al volo l'occasione dei virus per costruire dei programmi basati più su precise azioni di marketing che non su un servizio di ricerca e di assistenza degno di questo nome.

La parte del leone sul mercato finora l'hanno fatta i programmi di scansione, perché sono relativamente facili da implementare. Basati sull'assunzione che sia sufficiente identificare una «firma» per identificare un programma, hanno avuto un grande successo, che si è moltiplicato nelle due settimane antecedenti lo scorso 6 marzo, fino a far registrare incrementi del 3000% nelle vendite di alcuni prodotti. Tuttavia la maggior parte degli utenti li usa in modo piuttosto inconsapevole, e quasi tutti credono che sia sufficiente avere un buon antivirus per essere al riparo da sorprese sgradevoli. Il fatto che un programma di scansione debba essere aggiornato regolarmente per poter essere considerato efficace sfugge a molti utenti, come abbiamo rammentato anche qui sopra.

Proprio questa necessità di mantenere costantemente aggiornato il catalogo delle firme sta diventando un incubo per alcuni produttori. L'ultima versione di SCAN è cresciuta di circa 10 Kb rispetto alla precedente (poiché SCAN.EXE è compresso la crescita appare limitata a 7 Kb, ma se si espandono i due eseguibili, il precedente e l'attuale, si vede che in realtà le cose stanno diversamente). Probabilmente questa crescita non consiste interamente in firme di virus, ma è certamente significativa che in circa due mesi l'attività dei creatori di virus si è tutt'altro che rallentata; per avere un quadro completo della situazione occorre considerare il fatto che ormai i ricercatori perdono ben poco tempo sull'ultima versione di Cascade, Stoned o Jerusalem che continuano ad essere in testa alla hit parade dei virus, ma si concentrano su oggetti ben più minacciosi come ad esempio il Pogue, che è uno dei primi a far uso del MtE e che negli Stati Uniti è diffusissimo, o il Plastique 5.21 che promette (forse dovremmo scrivere «minaccia») di diffondersi ampiamente grazie alla sua struttura tripartita: si trasmette tramite i .COM, gli .EXE e i boot sector.

È ragionevole supporre che questa escalation debba prima o poi concludersi. Non si può rimanere sul mercato a lungo quando la propria strategia di marketing consiste in un infantile «il-mio-programma-riconosce-più-virus-del-tuo». La ragione per cui la tecnologia della scansione continua ad essere la più praticata è che costituisce la base della disinfezione dei programmi infetti, che in molti casi risulta l'unica possibilità per quegli utenti che, a dispetto di tutti gli avvertimenti, non hanno conservato integre le copie originali del proprio software, o magari non le hanno mai possedute. A molte aziende è capitato di farsi sviluppare programmi da software house che poi sono fallite, hanno chiuso o comunque non sono più in grado di garantire l'assistenza. Spesso queste software house installano i propri programmi con qualche dispositivo di protezione e non consegnano i dischi originali dei programmi medesimi; se i programmi sono di importanza vitale per l'azienda, ad esempio perché gestiscono la contabilità, la fatturazione o il database dei clienti, è comprensibile che l'azienda in caso di infezione voglia cercare di evitare di «distruggere i programmi infetti» come viene suggerito in questi casi, e voglia invece cercare di ripristinarne la funzionalità.

A chi si trovi in queste condizioni consigliamo, qualora non lo abbiano ancora fatto, di far effettuare il più presto possibile una verifica dello stato di salute di questi programmi; dopo averne accertato l'integrità si effettuerà un backup, da riporre in luogo sicuro al riparo da sorprese. Non tutti i virus infatti sono così ...«gentili» da consentire una facile disinfezione. Alcuni di essi modificano in modo irreversibile il programma vittima, e in questo caso non esiste potenza al mondo in grado di ripristinare il programma nel suo stato primitivo, e renderlo nuovamente utilizzabile.

Ma siamo certi che nonostante le nostre raccomandazioni ci troveremo spesso in condizione di dover assistere utenti vittime di infezione da parte di virus più o meno distruttivi, e in assenza di backup utilizzabili.

### *Un'alternativa alla scansione*

Abbiamo visto che mantenere efficiente ed efficace un programma di scansione sta diventando una scommessa. Ma esiste un'alternativa?

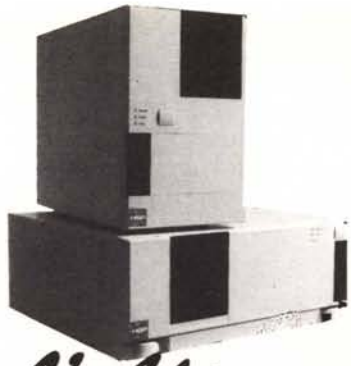
L'alternativa esiste e ne abbiamo parlato, seppure di passaggio, in un precedente articolo. Si tratta dei programmi di controllo dell'integrità dei file. Abbiamo ricevuto ultimamente un programma piuttosto interessante che appartiene a questa categoria; lo stiamo esaminando a fondo e ne parleremo in un prossimo numero, ma sin da ora possiamo anticipare che si tratta di una tecnologia le cui possibilità sono ancora da esplorare.

Il concetto è semplice. Un virus che si trasmette a un computer ne modifica almeno un file eseguibile, dove tra i «file» si possono far impropriamente rientrare anche il master boot record e il partition boot record. Un programma di controllo di integrità, correttamente utilizzato, è in grado di evidenziare immediatamente l'avvenuta modifica, consentendo all'utente di mettere in atto le misure di recupero che gli consentiranno di riprendere rapidamente il proprio lavoro senza ulteriori conseguenze, limitando al massimo la diffusione del virus. Sarà sufficiente dotarsi di un buon backup dei programmi eseguibili, che oltretutto non sarà necessario ripetere con frequenza perché si suppone che, al contrario dei dati che presumibilmente cambiano in continuazione, i programmi siano piuttosto stabili.

Diciamo subito che non si tratta di una misura da utilizzare in alternativa alla scansione, ma in aggiunta. Una scansione correttamente effettuata riesce a bloccare l'infezione prima che si trasmetta, mentre il controllo dell'integrità dei file la rileva subito dopo, cioè prima che possa diffondersi; ma abbiamo visto che in alcuni casi può essere già troppo tardi. Esistono infatti dei programmi che si installano sul disco fisso con un meccanismo non standard, utilizzato solitamente per la protezione contro le copie pirata. Alcuni di questi programmi non funzionano se ripristinati da un backup. In questi casi è necessario ricorrere al secondo dischetto di sistema, abitualmente fornito dal produttore che si avvale di una simile misura di sicurezza per il proprio software. La prima volta andrà presumibilmente tutto bene, ma se lo stesso programma dovesse nuovamente infettarsi potrebbe essere necessario acquistare nuovamente il prodotto. MCmicrocomputer si è espressa più volte contro l'adozione di misure di protezione così rigide, e non soltanto con riferimento ai virus.

In ogni caso la combinazione di un programma di controllo di integrità utilizzato congiuntamente ad almeno due distinti programmi di scansione fornisce la certezza dell'identificazione precoce di una eventuale infezione, e una ottima probabilità di recupero. Se a queste misure si aggiunge una regolare procedura di copie di sicurezza si ottiene la protezione ottimale, anche in termini di rapporto costi/benefici. MC

*Stefano Toria è raggiungibile tramite MC-link alla casella MC0170.*



COMPUTER
**HSP**
COMPUTER

# *L'Alternativa alle grandi marche*

DESIGNER - 21

## AT 16/21 MHz
## da L. 390.000

512K FDD 1.44 RS232 PRINTER

PROCAD-40

## 386 40 MHz
## da L. 790.000

1MB FDD 1.44 RS232 PRINTER

IPERCAD-486

## 486 33 MHz
## da L. 1.349.000

1MB FDD 1.44 RS232 PRINTER

### COPROCESSORI

## I VERI SALDI!!!

| | | |
|---|---|---|
| 80287-10 | L. | 99.000 |
| 80387-SX | L. | 199.000 |
| 80387-25 | L. | 229.000 |
| 80387-33 | L. | 229.000 |
| 80387-40 | L. | 229.000 |
| 487 SX | L. | 499.000 |

### HARD DISK

**VASTA GAMMA DA 40 Mb**
**A 1200 Mb**
## da L. 290.000

CD ROM INTERNO
**L. 499.000**

### SCHEDE GRAFICHE

**ANGOLO DEL CAD**

| | | |
|---|---|---|
| VGA 16 BIT 512K | L. | 99.000 |

**UVGA 32.000 COLORI ET 4000 AX**
1MB TSENGLAB L. 186.000

**NCR 1280 x 1024 2Mb**
**ACCELLERATORE WINDOWS**
**L. 259.000**

### MODEM

| | | |
|---|---|---|
| SK. 300/1200/2400 | L. | 99.000 |
| EST. 300/1200/2400 | L. | 149.000 |
| SK. 300/1200/2400 MNP5 | L. | 149.000 |
| EST 300/1200/2400 MNP5 | L. | 249.000 |
| SK MODEM/FAX 9600 63 | L. | 249.000 |
| **V.32 9600 BAUD** | | |
| HIGH SPEED MNP 5 | L. | 890.000 |

DESIGNER SX

## 386 SX 25 MHz
## da L. 549.000

512K FDD 1.44 RS232 PRINTER

IPERCAD-SX

## 486 SX 20 MHz
## da L. 890.000

1MB FDD 1.44 2RS232 PRINTER

IPERCAD-50 NOVITÀ

## 486 50 MHz
## da L.1.990.000

256 K CACHE MEMORY

### STAMPANTI

**CITIZEN**
**TUTTA LA GAMMA A PREZZI INCREDIBILI**

| | | |
|---|---|---|
| 224 D 24 AGHI (OPZ COLORE) | L. | 429.000 |
| SWIFT 24 X 136C 192 CPS | L. | 739.000 |
| SWIFT 24 E COLORI | L. | 569.000 |
| **NEC** | | |
| P20 80C 216S 24A | L. | 529.000 |
| **EPSON** | | |
| LQ 570 80C 225 CPS | L. | 649.000 |
| LX 1050 136 C 190 S 9A | L. | 649.000 |
| LQ 400 80C 150S 24A | L. | 449.000 |
| LQ 1070 136 C 225 CPS 24A | L. | 899.000 |
| EPL 4100 A4 6PPM LASER | L. | 1.450.000 |
| EPL 7500 A4 6 PPM PostScript | | TELEF. |
| LX 400 80C 150CPS 9A | L. | 299.000 |

**OFFERTA DEL MESE!!!**
**NEC 3 FG**
**L. 969.000**

### MONITOR

| | | |
|---|---|---|
| UVGA MONO 1024x768 | L. | 175.000 |
| VGA MONO PW PHILIPS | L. | 199.000 |
| UVGA COLORI 14" PHILIPS | L. | 580.000 |
| UVGA 14" COL. 1024x768 0.28 DP | L. | 449.000 |
| UVGA 17" COL. 1024x768 0.31 DP | L. | 1.490.000 |
| 19" COLORE 1024x768 I | L. | 1.790.000 |
| NEC 3FG | | TELEF. |
| NEC 4FG | | TELEF. |
| NEC 5FG | | TELEF. |
| PHILIPS 20" COLORI 1280x1024 | L. | 2.200.000 |

**OFFERTISSIMA**
**S.G.UVGA 16 BIT 1MByte**
**32.000 COLORI**
**+ MON. 14" 1024x768 0.28**
**L. 599.000**

## NOTEBOOK
## A4 kg. 2.8
**386 SX 20 MHz 2MB**
**HD 60 MB**
**L. 2.290.000**
**FDD. 1.44 RS232+ PRINTER**

## MULTIMEDIALE!!!
**SOUNDBLASTER V. 2.00**
**L. 199.000**

### ACCESSORI

**OFFERTISSIMA MOUSE COLORATI**
**L. 39.000**

| | | | |
|---|---|---|---|
| TAVOLETTA 12"x12" W/STILO | | L. | 290.000 |
| TAVOLETTA 18"x12" W/STILO | | L. | 520.000 |
| **PLOTTER ROLAND A3 → A0** | | | |
| **DA L. 1.490.000** | | | |
| SCANNER A4 MONO FLATBED | | L. | 1.990.000 |
| SCANNER A4 COLORI GT 6000 | | L. | 2.990.000 |
| HANDY SCANNER COLORI | | L. | 890.000 |
| DISCHETTI 1.44 | | L. | 1.100 |
| DISCHETTI 720K 3.5" | | L. | 585 |
| FAX PHILIPS | da | L. | 590.000 |
| STREAMER 250MB USA | | L. | 790.000 |
| **LOGITECH** | | | |
| MOUSE | da | L. | 75.000 |
| SCANNER 032/256 | da | L. | 199.000 |

**ECCEZIONALE!!!**
EPSON EPL 4100
LASER 6 PPM L. 1390.000

INFO.SIST.

*IL TUO COMPUTER*
*DI FIDUCIA*

CENTRO ASSISTENZA
TECNICA PC.

**ROMA - Via Endertà 13**
**Tel. (06) 8315076/8315083/8315093**
**MILANO - Via Vetta d'Italia 19**
**Tel. (02) 48193183/48013285**
dal Lun. al Sab. 9.00-13.00/15.30-19.30
**GARANZIA 12 MESI - PREZZI IVA ESCLUSA**