1993

Development of a classification system for computer viruses in the IBM PC environment using the DOS operating system

Hugh R. Browne
Edith Cowan University

Edith Cowan University

Copyright Warning

EDITH COWAN UNIVERSITY

PERTH, WESTERN AUSTRALIA

Faculty of Science and Technology

B.App.Sci.(Info.Sci.)(Honours)

Development of a Classification System For Computer Viruses In The IBM PC Environment Using the DOS Operating System

HUGH R. BROWNE
B.App.Sci(Info.Sci.)
P.O.BOX 564. BUNBURY.
WESTERN AUSTRALIA 6230.

Principal Supervisor: Associate Professor
A.Watson

Other Supervisor: Mr. T. Haines

Semester 2, 1993

USE OF THESIS

The Use of Thesis statement is not included in this version of the thesis.

ABSTRACT

The threat to computers worldwide from computer viruses is increasing as new viruses and variants proliferate. Availability of virus construction tools to facilitate 'customised' virus production and wider use of more sophisticated means of evading detection, such as encryption, polymorphic transformation, and memory resident 'stealth' techniques increase this problem. Some viruses employ methods to guard against their own eradication from an infected computer, whilst other viruses adopt measures to prevent disassembly of the virus for examination and analysis. Growth in computer numbers and connectivity provide a growing pool of candidate hosts for infection.

Anti-virus workers have developed individual methods of classifying and naming viruses. Diversity of approaches has resulted in ambiguity and confusion in many cases.

Standardised and flexible systems for classification and naming are needed to eliminate ambiguity and to promote effective identification of viruses. This study is an examination of one candidate classification method. A depth-mediated variation of monothetic analysis has been developed to classify a database of virus information stored in binary variables. The

method trialled in this research is suitable for use, although generalised application of monothetic analysis is limited, as only binary (Boolean) variables may be analysed, whilst some pertinent virus information may be of a numeric or descriptive type.

The storage of the virus information in a database allows for flexibility in both data volume (new virus reports) and virus characteristics (new variables). Items in both of these categories may be easily added to previously stored information.

The data which was used for this study, however, although suitable as test data for the proposed classification technique, is inadequate for taxonomic classification purposes, being highly variable in format, content, and completeness. Several questions also arose regarding accuracy. Such deficiencies were disregarded for the purpose of this study as it was possible to verify in all cases that no current category of virus was missed (omission of which would have made the trial data incomplete).

Secondary objectives for this study were the consideration of a suitable nomenclature, resolution methods for delimitation conflicts, and a classification encoding method.

Currently, the name of a new virus frequently includes the name of the perceived parent virus. The solution to the problem of variations in naming will depend on whether this 'patronymic' system is continued. Increases in variability and identification problems caused by encryption and particularly polymorpism may make long term continuation of this approach impractical.

Mediation for delineation conflicts, is met by the classification system itself, as the group into which a virus falls is determined by its possession of the requisite characteristics.

An encoding method for virus classification details has been provided by the progressive building, during classification, of a node identifier for each virus record, which identifies the branch conditions carried out to group that virus. This provides the variable names on which the virus has been grouped, and together with the values for each of the variables used, summarises the virus characteristics in terms of the classification variables and the depth to which classification has proceeded.

Declaration

I certify that this thesis does not incorporate, without acknowledgement, any material previously submitted for a degree or diploma in any institution of higher education and that, to the best of my knowledge and belief, it does not contain any material previously published or written by another person except where due reference is made in the text.

Signed

ACKNOWLEDGMENTS

SIncere thanks are due to my supervisors, Associate Professor Anthony Watson, of the Mount Lawley Campus of Edith Cowan University, Perth, Western Australia, and Mr. Terry Haines, of the Bunbury Campus of Edith Cowan University, Bunbury, Western Australia for their support and advice during this study.

TABLE OF CONTENTS

List of Tables and Figures

Tables

Figures

CHAPTER 1 - INTRODUCTION

Justification

Many authorities in the computer virus field have pointed out the acceleration in the rate of virus occurrence during recent years. Although there is some dissent about the precise rate and projections into the future, there is general agreement that more efficient prevention and detection methods, as well as methods of damage minimisation, are required.

Cohen (1986, p.1), was one of the first to point out the vulnerability of computers to viral attack. He also demonstrated that the potential evolutionary characteristics of viruses (the 'mutation' into any computable sequence) endowed them with Turing capability, suggesting that random alterations to viral code caused by variations or faults during propagation could produce an evolutionary trend in viruses which could accelerate as they became more widespread. Many models of exponential propagation and infection have been demonstrated: **Fites, Johnston and Kratz (1992, p.27)** suggest that in an environment where both high exchange of information is taking place, and large numbers of users are available for infection, as many as 17, 000, 000, 000 infections could take place within the first 49 hours of activity. **Kamay and Adams (1992, p.12),** observe that computer viruses constitute 65.8% of computer abuse cases reported in Australia during the period reviewed in their report (June 1990 - October 1991).

Others have scrutinised the current computing environment to identify the root causes of the proliferation of the malicious code. **Caelli, Longley and Shain, (1991, p.590),** have argued that fundamental features of the von Neumann architecture (specifically, the equal treatment awarded to data and programs) are key weaknesses which are exploited by virus authors and their code.

The DOS operating system is blamed by **John McAfee (1992, p.30)**, on the other hand, for the flourishing number of viruses which are found in the IBM PC/DOS environment. Whilst other operating systems are not immune from such attacks, it is also clear that the vast majority of current viruses are specific to the DOS environment. There is no doubt that the widespread use of DOS has fostered software development and interchange on an international scale, and that this, in turn, has created a fertile environment for virus proliferation. The current study focuses exclusively on the area of DOS viruses, in the belief that these will provide a representative cross-section of computer virus types which occur in all environments. It is also clear that the burgeoning growth in connectivity worldwide will provide an ever larger and more accessible pool of potential victims for computer viruses.

The rapid growth in new viruses and variants has provided a growing problem for anti-virus product manufacturers, as existing 'pattern searching' detection methods are becoming increasingly cumbersome to maintain and

use, and progressively less effective. New variants which avoid existing detection patterns, on the other hand, are becoming easier and quicker to produce, with the use of ready made virus construction kit, reverse engineering, polymorphism, and variable encryption all currently increasing.

In summary, the increasing ease with which computer viruses may be produced or modified is resulting in increasing numbers of new viruses and strains of older viruses. Simultaneously, more sophisticated means of concealment are being used to prevent detection and/or removal of virus infections. Consequently, anti-virus products require constant updating and improvement and the manufacturers of such products are under some pressure to continuously produce timely responses to new or altered viruses. Differing avoidance, detection and eradication methods have also evolved, and while diversity of method is to be encouraged, access to centralised and standardised information about new threats may result in quicker and more efficient activation of countermeasures.

A more serious deficiency in the current situation is the divergence in classification and naming standards. During the current study cases of both synonymy (multiple names for one virus) and homonymy (multiple objects with the same name) have been found. Many cases have also occurred where viruses described by one authority does not correspond to any description from another authority. This makes it difficult, if not impossible, to verify that any particular virus which is detected by one product will be

detected by another product although both may list the same virus name as one which their product effectively detects. Lack of standardisation also hampers efficient notification of virus incidents and occurrences, and may also lead to confusion and lowered vigilance amongst the public.

Objectives of this study

The objectives which this study seeks to address is to develop an unambiguous, extensible and modifiable classification system for computer viruses in the IBM PC/DOS environment, using monothetic analysis on binary variables representing the presence or absence of particular virus characteristics.

Additional goals to be considered

1. To suggest a standard nomenclature for IBM PC/DOS computer viruses.
2. To suggest a method of mediation for delimitation conflicts, which will provide clear guidelines to determine whether a particular virus is a variant of an existing type, or a new type which should be considered distinct.
3. To provide an encoding method for significant virus characteristics in a way that will allow an accurate and meaningful summary of characteristics used in the classification to be deduced.

Significance of the study

In view of the problem presented by the continuing increase in the number of viruses at large, the increasing ease of virus production through dissemination of virus code and production tools, the growth in connectivity and data transfer and the decline in effectiveness of pattern matching methods of detection, the need for new and more efficient means of virus detection and prevention is increasing.

Currently available information about computer viruses from varying sources has resulted in differing interpretations of similarities and differences, some of which are superficial characteristics which may easily change, either by natural variation, or by minor alterations.

As pointed out by **Blackwelder (1967, p.218)**, taxonomic classification systems require resolution of both synonymy and homonymy. To detect instances of these problems, it is necessary to determine with certainty whether a particular item for classification is of a type which has already been classified. To make this possible, a standard method of classifying viruses is needed to allow comparison of virus characteristics , as well as enabling the development of generic detection and eradication measures.

The current study is a trial implementation of one candidate method for grouping viruses according to the values of binary variables (variables which denote either the presence or absence of a characteristic).

Reasons for selection of data from sources used

Several possible sources of data were evident at the stage when the research proposal for this thesis was prepared; those to hand, however, were dated and appeared to be either extracts from other sources or incomplete. The primary source of published information at that time was Patricia Hoffman's ***VSUM***, which deals with the international incidence of viruses, but is based in the United States, This list is periodically updated, Another reliable source of information was identified as the monthly publication ***Virus Bulletin***, which provides information on virus occurrence, as well as details of new virus strains reported, primarily for the United Kingdom and the European area. When a copy of ***VSUM*** was obtained and the ***Virus Bulletin*** data examined, these two authorities were identified as the major sources from which other published summaries had been derived. These findings are discussed in more detail in the section describing Data Sources.

Reasons for selection of data storage used

A database was chosen as the method of storing the captured data. This was not because a database is the only, or necessarily the best, environment for programming and carrying out a statistical analysis of this type. In fact, if monothetic analysis was the sole objective, a special purpose program to perform the analysis on the data would have been the preferred approach. There were also peripheral questions for determination

in this study, however, and these required detailed scrutiny of the information held in existing systems and the methods used for naming, classifying, and grouping this data. One such area was the matter of nomenclature, which is an inherent component of any standard classification system. Considerable divergence and some controversy was evident in the approaches adopted by the two main data sources, ***VSUM*** and ***Virus Bulletin***. This dissent existed largely over whether particular viruses should be recognised as variants of existing strains, or entirely new types.

A customised analysis program using limited binary variables would not be satisfactory for examination of wider characteristics, where much of the data is either not binary (and could not be meaningfully reduced to binary data by techniques such as 'clumping'), or is of a qualitative nature and only easily expressed in text descriptions. However, it was still necessary to accumulate data which could be of interest, to determine its content, consistency, completeness, and suitability for analysis. The accommodation of changes to the data for analysis would also present problems for customised programs, which could require changes to the program code, requiring both user access to the program source code and user proficiency in the programming language in which the program is written. This problem was acknowledged by Kaufman et al (1990, p.303), where the need for user modification of array sizes is pointed out if the data to be analysed contains more than 100 objects. The database approach used in this study is free of this restriction.

For flexibility and varied analysis, therefore, a database was used to accommodate all data collected, and a reduced subset of the gathered data, consisting of identifiers and binary variables only was used as source data for the monothetic analysis program.

The decision to use a database imposed some constraints in itself, which are further described in the Chapter 3, under the subject Software Limitations.

Reasons for selection of the analysis technique used

Most of the information collected consisted of non numeric variables and many of these were already of a binary type. The variables pertinent to the identification and analysis, for which values were sought for each virus, are listed in Table 1 below.

A small number of additional details were also collected to assist in identification of corresponding viruses where names allocated by different authorities differed. These included date of original occurrence, origin, status (e.g. common, rare, extinct).

Variable	Description	Data type
NAME	Listed virus name	Text
RES	Whether virus gains memory residence	Binary
MBR	Whether virus infects Master Boot Record	Binary
COM	Whether virus infects executables with .COM extension	Binary
EXE	Whether virus infects executables with .EXE extension	Binary
OVL	Whether virus infects executables with .OVL extension	Binary
SIZE	Infective size (increase in infected file length) in bytes	Num
EFF	Description of discernible effect(s) on activation	Text
REPLIC	Description of replication method	Text
DOSBOOT	Whether virus infects DOS boot sector	Binary
FD	Whether virus infects diskettes, exclusively	Binary
CMD	Whether virus infects command processor	Binary
O_W	Whether virus infects by overwriting host program code	Binary
PSITE	Whether virus infects by parasitising host program	Binary
SPAWN	Whether virus creates companion .COM file	Binary
FAT	Whether virus infects File Allocation Table	Binary
PART	Whether virus infects Partition Table	Binary
TRIG	Trigger condition if known	Text
AKA	Alternative name(s)	Text
STEALTH	Whether stealth methods used for detection avoidance	Binary
ENCRYPT	Whether encryption used for detection avoidance	Binary
INTS	Interrupts utilised	Text
INFNO	Number of infections attempted for each activation	Text
VARS	Number of reported variants	Num
INFMODE	Steps used to carry out infection	Text
FILELOC	Viral code location within infected files	Text

Table 1: Variables collected during research

Some characteristics of interest (for example, the variable INFNO) could be reduced to values of a binary nature by use of the 'clumping' method. For the INFNO variable, most (95.4%) of the values belonged to one of:

1. Single candidate file infected;
2. Two candidate files infected;
3. Three or four candidate files infected;
4. All candidate files in current directory infected;
5. All candidate files in all directories infected.

Of the values which did not fall within one of the above categories, 3.9% of values were indeterminate (either unstated or unclear). The remaining 0.6% could not be quantified in terms of absolute values, resulting in only occasional infections, proportional infections (e.g. 50% of candidate files), or infection proportionate to the number of activations (infection every 10th virus activation).

It would therefore be possible, if infectivity were to be used as a criterion for analysis and the data was complete and explicit, to represent such values as the ones illustrated above as binary variables (with the exception of the 0.6% which were unquantifiable) by providing a binary variable for each category or 'clump'. A problem which could arise from extensive use of this technique could be the creation of artificial groupings. To provide effectively for all possible values, a relatively large number of binary variables must be used. However, each virus record may only contain a positive value for one of the new variables, being the 'clump' into which the variable value falls. This introduces a weakness in that the variables are

not fully independent of each other. A corresponding implication is that each of a group of 'clumped' variables will only contain definitive information about a percentage of the data, and the larger the number of 'clumps', the (potentially) smaller the percentage of records represented.

This artifice could result in bias during analysis, and would definitely cause deterioration in the already extensive processing time, due to the increase in the number of variables used. Manipulation of non-binary variables was therefore avoided in this study.

It was decided, because of the good number of true (unclumped) binary-type variables in the data, to seek an analysis method suitable for use on these values. Two immediate possibilities arose.

Kaufman and Rousseeuw (1990, p.22), describe the application of numeric clustering techniques to an intermediate data matrix produced by the computation of dissimilarity coefficients from a binary data set. This technique relies on two separate processes, the first preparing the intermediate data matrix to which the analysis process may be applied.

Also described by **Kaufman et al (1990, p.280)**, is the single step monothetic analysis method for clustering of exclusively binary data. Monothetic analysis is designed to operate directly on a matrix of binary data, so avoiding the extra computation of a prerequisite dissimilarity matrix.

As the initial examination of the data indicated that a large number of virus characteristics could be represented by use of binary variables, the choice was made to use the binary (or 'logical') data type offered by databases for storage of the data and to apply the principles described by **Kaufman et al (1990, p. 298)** to perform a monothetic analysis trial on the data.

CHAPTER 2 - METHOD OF DATA COLLECTION

Method of data collection

The version of ***VSUM*** from which the sample data was drawn uses 59 generic virus typecodes (disregarding subcategories such as indicators of the specific area of memory used). The ***Virus Bulletin*** recognised only 24 distinct codes (including reports up to, and including August, 1993)

The whole of ***VSUM*** was read, and the names of the viruses listed were entered to the database together with as many variable values about their characteristics as could be extracted from their descriptions. Where a particular entry was either not clear, or ambiguous, reference was made to other information sources in an attempt to resolve the question.

Considerable time was spent reading through variant descriptions, which are listed in text under the 'parent' virus name, to ensure that no new virus types were missed. As the information is in text format, the content, detail and coverage of descriptions varied widely, and variable values and information were often lacking altogether.

After completion and checking of the data entries, each virus type was matched to its predicted equivalent for the types included in ***Virus Bulletin*** listings. The actual virus types for each listed virus were then entered from

Virus Bulletin, starting with the updated list of all reports which was issued in July 1991, and adding the data from each successive monthly issue of the publication up to August, 1993. The predicted types (derived from the ***VSUM*** data) were then compared to the ***Virus Bulletin*** types. Many contradictions were evident between the ***VSUM*** descriptions and the ***Virus Bulletin*** entries.

For the purpose of this thesis such variations were not considered significant. As the objective is the demonstration of a classification system, the consideration of overriding importance was that all existing virus types were represented. The philosophy that was adopted to accommodate variations such as those described above was to ignore the difference, as long as a new virus type was not being overlooked.

Further discussion of perceived deficiencies in the data is conducted in Chapter 3, Limitations under the section Data Suitability.

Data Sources

Five authorities were considered as sources of data:

Fites P, Johnston P, and Kratz M (1992)

Levin R B (1990)

Hoffman P (Oct 1992)

Burger R (1988) and (1991)

Virus Bulletin (July 1991 - March 1993)

The first two sources (**Fites et al (1992)** and **Levin (1990)**) , were found to be extracts from an earlier version of the third source (**Patricia Hoffman's *VSUM***). Consequently, their data has been relegated to the status of reference material, in favour of the more current version of ***VSUM***.

Another source, **Hruska, J (1990)** was also considered, but it was found that this data was an early copy of ***Virus Bulletin***'s published lists, and this source was also retained as a reference source only.

The listings published by **Burger, R (1988 and 1991)** lack the detail, precision and coverage required for this study. Some material where conflict existed between ***VSUM*** and ***Virus Bulletin*** was been checked with Burger's texts which provided no additional information. His listings have therefore been disregarded.

It is also evident that both of the primary data sources mentioned above, **Hoffman, P (1992)** and ***Virus Bulletin*** edited by **Ford, R** provide information for public distribution and information, and that the organisation of the information is aimed at identification and detection rather than research. For this reason, it is probable that information suitable in both content, detail, accuracy and completeness for the extended analysis of

virus characteristics will only be produced by custom collection of data focussing on the required variables and format. In view of the large number of viruses already recorded, starting from the beginning may prove impractical or impossible. The following reasons may represent some of the hindrances to this type of study:

1. Obtaining a complete set of specimens would be difficult, and possibly undesirable, considering the need to limit by all possible means the further dissemination of viral code;
2. Disassembly and individual classification of such a large number of viruses would be extremely difficult and time consuming unless automated tools could be provided to assist;
3. As has been found in this study, variation in descriptions of one virus between different reporting centres is commonplace. This may arise from 'evolutionary' transitions of one kind or another (for example, changes in length resulting from extensive copying between different media where some media may 'clip' the code due to storage constraints or flaws). This type of change was suggested by **Cohen, F (1986)**, as a source of variability in virus strains.
4. Tools for automated examination and detailed classification are not widely available and would have to be obtained or designed and constructed de novo;
5. A 'clean' and secure environment would be required to ensure that research specimens do not escape.

Data Volumes

In all, 1513 viruses and virus variants were considered, listed under 730 main virus names. After corrections had been carried out, a total of 1497 viruses of 59 different types were identified. The typecodes used by ***VSUM*** provide the most detailed description codes available from the sources examined.

This figure is somewhat short of the number predicted at a conference in February 1992 by J. McAfee, when the number of existing viruses was given as approximately 1200 and the prevailing rate of increase as "2 to 3 per day". In fact, the increase rate, based on the above starting point and the data examined for this thesis, averaged out at a point closer to 1 (1.15) per day. This more moderate rate nevertheless illustrates the seriousness of the situation.

Data Collected

The information gathered was, in fact, in excess of that required purely for the grouping study which is the theme of this study. The method to be used (monothetic analysis) requires that the variables on which the grouping is to be based are of a binary nature - they may have one of only two possible values. Much of the information gathered (such as textual descriptions of the individual trigger conditions which have so far been identified, and discreet numeric variables such as the infective length of the virus, or the

number of individual infections a virus will attempt during each infection episode), are not suitable for use in monothetic analysis, even if reduced to a large number of binary variables by the use of 'clumping'.

The more detailed descriptions from ***Virus Bulletin*** were utilised, where possible, to resolve outstanding discrepancies; however, because of the relatively small number of viruses for which this high grade description is available, the benefits from this comparison were limited. The ***Virus Bulletin*** detailed descriptions provide an excellent source of 'in-depth' detail for the limited list of published analyses.

Data Currency

The ***VSUM*** version used as the primary data source was version X210, dated October, 1992. ***Virus Bulletin*** has been checked for data up to the August 1993 issue.

Unfortunately, the Hypertext format of the ***VSUM*** data makes it necessary to read each virus description in detail to extract some of the characteristics required for this study. Many characteristics, such as the intra-file location (which may evaluate as Prepend, Append, or Insert), for instance, as well as the number of infections per cycle, and activation details, are embedded in the text description for each virus.

New virus strains are not readily identifiable, either. The access mode and cross-referencing provided is based on virus names, and no provision is made for the report date or selection of a group based on date of report. This requires examination of each virus description header to determine the date of receipt, or at very best, a comparison of an existing virus name list with the ***VSUM*** index for each alphabetical letter, to determine whether a particular virus has been processed already.

The case of virus variants is worse still. The ***VSUM*** listing includes descriptions for variants of a particular virus at the end of the virus strain description. It appears that new variants are added to the list. The descriptions for these variants are abbreviated, varying in detail, and frequently omit items such as intra-file locations and the number of infection per cycle. In the absence of direct evidence to the contrary, it has been assumed that these 'child' viruses have inherited the characteristics of their 'parents'. The location of these variant listings, moreover, make it impractical to continuously update data, as this would require the re-reading of every virus description from beginning to end, comparing each entry to existing data to extract any amendments. An illustration of the difficulty involved is clear when considering viruses such as Jerusalem - 39 variants and 320 lines (5 A4 pages) of description, or Vienna - 24 variants and 216 lines of description. Relying on re-reading to identify changes in such volumes of text would not only be impractical from the time point of view, but extremely error prone.

Correlation of Data from Different Sources

Although a reasonable number of virus descriptions from ***VSUM*** initially matched ***Virus Bulletin*** reports, there was, as has already been stated, disagreement on detail in many cases. It was expected that the number of viruses where the description had appeared in ***VSUM*** but not in ***Virus Bulletin*** would gradually decrease because no new data was to be entered from ***VSUM***, whilst new data from ***Virus Bulletin*** was to be continually checked for correspondences.

However, many of the original discrepancies remain, and later ***Virus Bulletin*** reports contain increasing numbers of viruses which were not identifiable as viruses already reported by ***VSUM***. The latest ***Virus Bulletin*** reports contain no correspondences with outstanding ***VSUM*** data. There are, as at August 1993, of the 730 ***VSUM*** virus strains, still 236 not matched to ***Virus Bulletin*** reports. Of these, 101 were reported by ***VSUM*** in 1991 or before. This would appear to indicate that some viruses have a limited spread, and are localised to a specific area. To some extent, the discrepancy may be attributable to differences in naming or classification, and the data used here does not contain the detail that would be required for a full statistical analysis of the epidemiological trends which I have suggested may exist.

The following graph shows the divergence of correspondence between the sources:

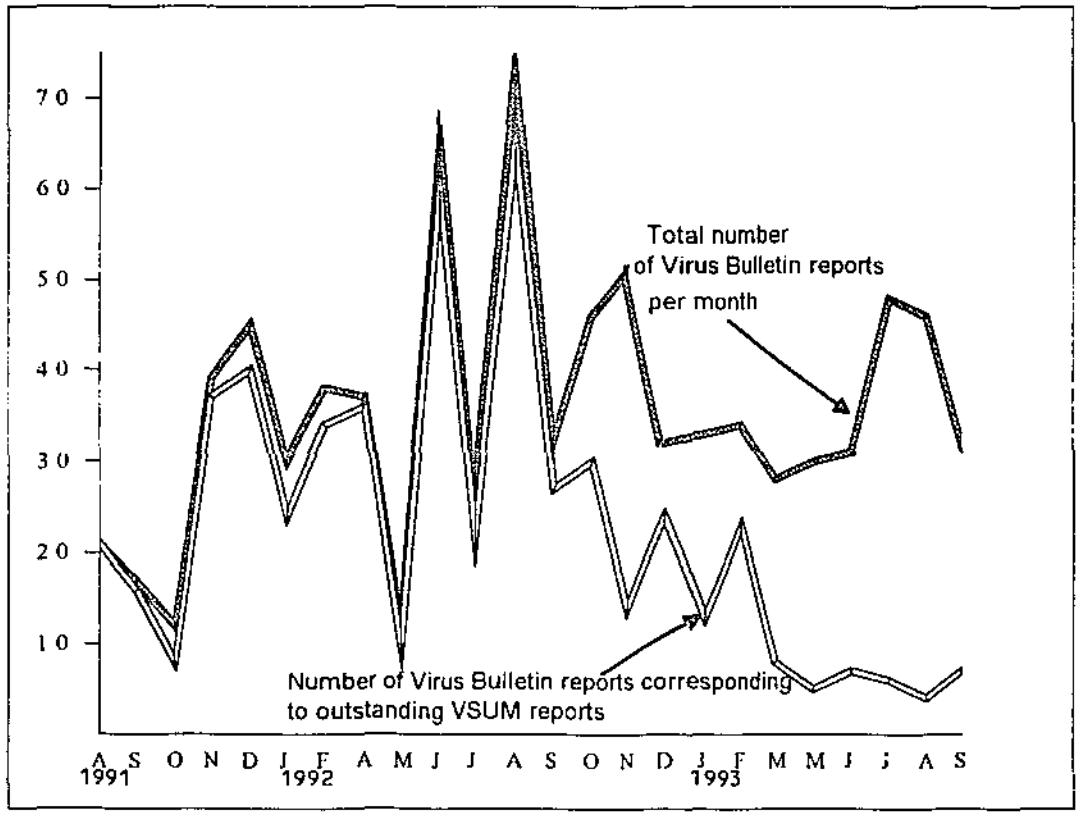

Figure 1. Correspondence of total new reports in Virus Bulletin to outstanding VSUM items
(March 1992 and April 1993 Virus Bulletin reports were not available)

CHAPTER 3 - METHOD OF ANALYSIS

Data Stored

The data used for the trial analysis consisted of a subset of the data collected from ***VSUM***. The selection was based on all records and a select number of fields which contained binary data. Although efforts were made to correct this data, there may be residual mistakes in the detailed field values arising from incomplete or ambiguous data. The data in this database has been reduced in volume to approximately one tenth of the data collected. This reduction serves as the type of data reduction described in **Miles and Huberman (1984, p. 21)** but also has the convenient effect of reducing the amount of memory required for processing. Nevertheless, the analysis process requires considerable time; the processing for the results displayed here required nearly one hour, running on a computer with an Intel 486DX processor operating at 50 MHz with 4 Megabytes of RAM. Although this time may seem excessive, **Kaufman et al (1990, p.272)**, give computation times for a divisive analysis using 100 records and only 2 variables as 6.65 minutes. Using, as has been done in this study, 730 records and 7 variables (requiring approximately 20 times as much processing), it is acceptable that the processing time should increase at least tenfold, although considerable optimisation of the process may still be possible.

Comment has been made on the unsuitability of this data for serious research, in Chapter 3 - Limitations, under the section Data Suitability. However, the data used here will give a real demonstration of the function of the monothetic analysis technique, when used with the type and volume of data arising from virus descriptions. The data used for analysis has been included as Appendix A.

Database structure

The total processing package consists of three databases: the main storage database, named VIRBIN, containing the virus names and descriptive values, in the form of binary variables. Also contained in this database are fields to record the classification status progressively awarded to each virus during processing, according to the cluster of data into which the virus falls at each division.

The other two databases are control databases, the first of which (MONOFLDS) is used to hold temporary results of the similarity coefficients for variables, so that, for each pass, the maximum culminating value may be selected as defining the most centrally located variable of those scanned, and this variable used as the division criterion for the pass. The contents of the MONOFLDS database are included as Appendix C.

The second of the control databases, NODEVARS, stores the details of the progressive splits which are carried out, the branch criteria values, and details of the usage of variables, so that the use of a variable to carry out a split of the data will preclude its reuse as a classification variable in all descendant branches of the binary tree produced. The number of records in this database determines the depth to which the main database will be split. The contents of the database are provided as Appendix D.

Algorithms used

General Monothetic Algorithm.

The monothetic algorithm described by **Kaufman et al (1990, p.298)** successively selects the most centrally located variable from those available, and splits the data into two groups: those that possess the characteristic and those that do not. Each of the resulting groups is then processed independently to determine the most centrally located variable within that group. Variables that have been used to split the data at an ancestor node may not be reused at lower levels, but otherwise the use of variables is unrestricted, and either the same or differing variables may be used to split the data at sibling (same level, different branch) nodes. In the Kaufman model, splitting continues until a split produces a single indivisible object, all variables have been used, or until remaining variables are unable to provide any further splits. The technique used in this study follows the same technique, apart from the termination conditions.

The method used to compute the most centrally located variable is that each variable is examined and scored against every other available variable according to the following method:

	TRUE	FALSE
TRUE	a	b
FALSE	c	d

Figure 2: A general two-by-two contingency table

In respect of the example contingency table above, the calculation of a variable score for a variable ***f***, in relation to all other variables, ***g***, using the method proposed by **Kaufman et al (1990, p.306)** is expressed mathematically as:

$$\sum [a_{fg}d_{fg} - b_{fg}c_{fg}]$$

This may be stated descriptively as:

> ABS((occurrences where both variables are TRUE * occurrences where both variables are FALSE) - (occurrences where var1 is TRUE and var2 is FALSE * occurrences where var1 is FALSE and var2 is TRUE))

Application of the absolute function to the computation results in the removal of negative values.

Score calculation may be demonstrated in a two-by-two contingency table containing sample data:

		Variable 2	
		TRUE	FALSE
Variable 1	TRUE	17	23
	FALSE	10	55

Figure 3: An example of a two-by-two contingency table with sample data

The similarity score for the above scenario may be computed as:

ABS((TRUE/TRUE * FALSE/FALSE) - (TRUE/FALSE * FALSE/TRUE))

evaluating to: ABS((17 * 55) - (10 * 23)) = 705

The effect of different variable values on the overall score may be seen in the following examples:

	TRUE	FALSE
TRUE	200	200
FALSE	200	200

Figure 4: An example of evenly distributed variable values

The variables immediately above will provide a NIL score, as the values are equally distributed for association and difference.

Evaluation: ABS((200 * 200) - (200 * 200)) = 0

	TRUE	FALSE
TRUE	390	10
FALSE	10	390

Figure 5: An example of data with strong association

The above variable values would provide a high score:

Evaluation: ABS((390 * 390) - (10 * 10)) = 152000

If the two variables possess values which are perfectly opposed, (i.e. var1 is always TRUE when var2 is FALSE, and var1 is always FALSE when var2 is TRUE), the association will be as high as when the variables are perfectly matched.

	TRUE	FALSE
TRUE	0	400
FALSE	400	0

Figure 6: An example of data where all values are opposing

As the variables have opposite values for all records, the measure of association is perfect.

Evaluation: ABS((0 * 0) - (400 * 400)) = 160000

It has been noted by **Kaufman et al (1990, p.282)** that this measure of association closely resembles the chi-square statistic for the two-by-two

table. The selection of the variable that has the highest similarity to all other variables means that the chosen variable will, in fact, be the most centrally located in the set of variables compared for the pass.

Following the selection of the best variable for use to divide the data, the data is divided into two sets, containing records which have a TRUE value for the variable, and those which have a FALSE value for the variable. The variable evaluation process may then be repeated independently for each of the new groups, which may be redivided, and so to completion of the analysis.

As the classification proceeds, the completed partitioning steps will progressively produce a binary tree form. A binary tree has the characteristic that any parent node may only have two child nodes, and any node must have one and only one parent node (excepting the origin, or root node, which has no parent). A diagrammatic representation of the completed classification, showing intermediate steps and branches, follows:

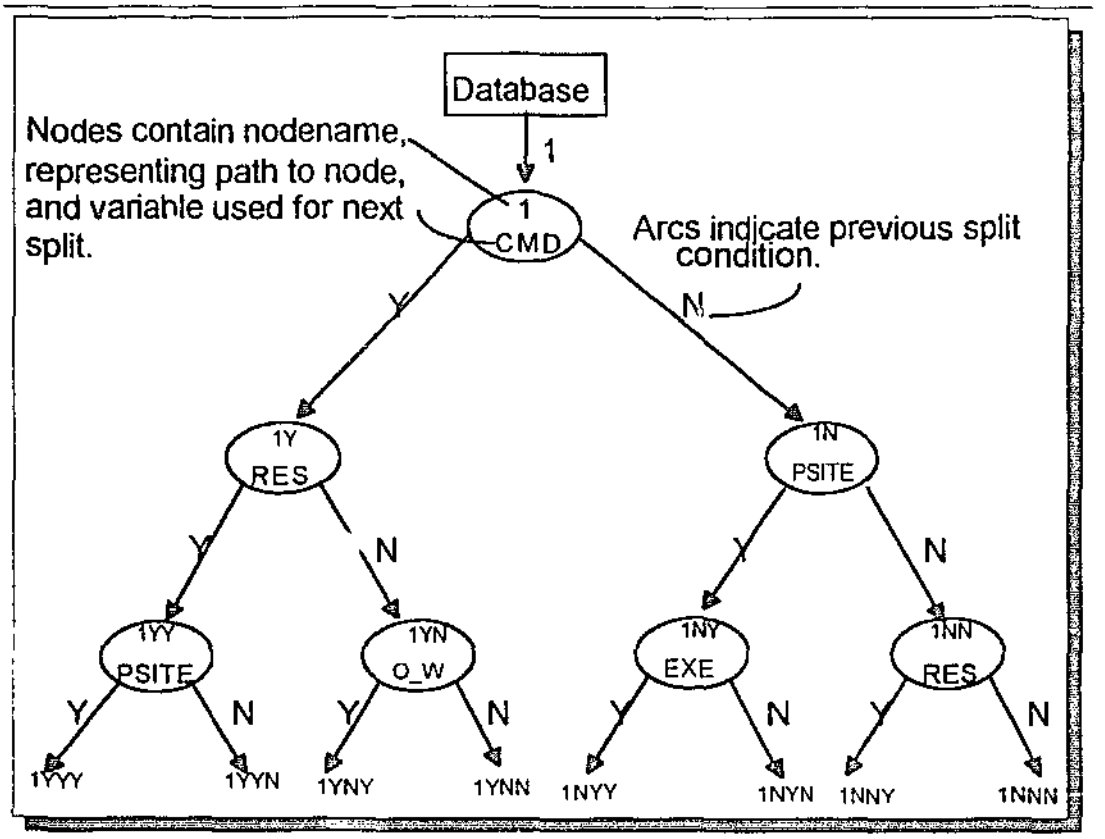

Fig 7: Illustration of the binary tree formed by monothetic analysis

The method used in this study follows the model suggested by Kaufman et al, except in the matter of termination conditions. Instead of requiring the analysis to proceed until the smallest possible partition has been achieved, as is the case in the Kaufman model, the NODEVARS database has been used to control the depth to which the partitioning is to be carried out.

This has several practical advantages. It allows more control over the partitioning process, as it is not necessary to include all variables available in the data in the processing. It is also possible, with minor modifications to the program, to extend a previous classification to a greater depth, saving

considerable processing. The degree of detail (and therefore the granularity of the resultant groups) in the partitioning is also controlled, by specifying, in the NODEVARS database, the maximum depth (number of levels) to which the partitioning may proceed. From the development and testing point of view this was also crucial, as the extended processing duration necessary to carry out a full analysis following the method described in **Kaufman et al (1990, p.280)** using every available variable would be unacceptable.

The partitioning achieved using the method adopted in this study will also, because it is depth-mediated, result in a balanced binary tree.

The modified method also has some disadvantages, however. It requires that a minimum number of variables are available to carry out an analysis to its required depth, although not all may necessarily be used. The number of variables required is, because of the preordained form of a binary tree, directly related to the depth specified. The relationship may be specified as:

$$N = 2^{(depth)} - 1$$

where N represents the required number of variables, and ***depth*** is the number of levels required. Thus, for an analysis to complete the third level of depth (allowing partition into 8 subgroups, as in the preceding figure), a minimum of 7 variables must be provided, and these must be present in both the MONOFLDS and NODEVARS databases. However, not all variables must be used; the use of identical variables in independent branches of the tree means that some of the required variables may remain unused. If this

prototype were to be adopted as a functional classification method where depth could be specified by the user, some validation would be necessary to ensure that the number of variables provided is adequate for a partition to the requested depth.

Database program algorithm.

The database program itself is provided as Appendix E. In broad terms, the analysis process follows the following logic:

```
For each node, in sequence, specified in depth control database
    Read variable availability details from depth control database
    Load variable availability details for the node into processing details database

    For all available variables for node in processing details database, use as PRIME
        For each PRIME, pair with every available variable as SECONDARY
            For every record in main storage database
                Compute similarity score
                Add to similarity score for variable pair
            Store total score for variable pair in processing details database
        Rezero variable scores
        Select next candidate as PRIME
    Choose highest similarity score of all PRIMEs as split variable for node
    Update depth control database with node usage, variable usage, and node split
        information
    Update all records in main storage database records with node split information
    Move to next node
```

If two variables both produce the highest similarity score, the program will, by default, choose the first listed of the variables (in the record order of the MONOFLDS database) as the variable on which to partition.

The program also displays progressive summaries of the processing results calculated from the similarity scores and the selected partitioning variable for individual passes as the processing takes place. A sample of this display is included as Appendix F.

CHAPTER 4 - LIMITATIONS

Software Suitability

A relational database was the storage method chosen for the data gathered, because of the flexibility offered for data manipulation, analysis, and reporting.

Several problems arose from this choice. A functional prerequisite for the database was the ability to use indirect addressing. Specifically, the field names of the main storage database were required to be stored in other databases, to allow flow control of the analysis process and storage of the progressive analysis results. The field names stored in the control databases as data were then required to be used to address the data in the relevant fields in the main storage database. Although this feature appears simple, only one database of several candidates documented the feature as available. This was the relational database of the integrated package, ENABLE, version 4.0, although the implementation of indirection that was offered was somewhat limited and necessitated some convoluted syntax through the use of 'ELSE' clauses to achieve what should have been a simple negated conditional. ENABLE, however, offered only one-dimensional arrays which were not suitable for intermediate result storage.

The method of analysis, which carries out repetitive passes to assess the strength of similarity between pairs of variables, could be considerably

optimised by the use of a two-dimensional array to store the results of previous pairings so that these results could be used to minimise the calculations as the analysis progressed. For example, if variable A is paired with variable B and the similarity between these two variables established, the same result will apply to variable B paired with variable A later in the same pass.

In weighing these two conflicting requirements against each other, the requirement for indirect addressing was found to be essential to the success of the database program design, whereas the desirability of two-dimensional arrays was required for optimisation only. This finding militated in favour of the use of ENABLE.

An additional advantage of the selection of the ENABLE software was the support of ANSI level 2 SQL statements embedded in ENABLE'S procedural database language. This permitted the use of powerful non-procedural SQL instructions with a considerable reduction in code complexity in some cases.

Data Suitability

The content and format of the data proposed for use in this project were not known at the time of preparation of the thesis proposal. Completeness and consistency, moreover, was not evident until considerable data had been captured from ***VSUM*** and trends had become apparent. Because of the

informal textual nature of much of the data, it is difficult or impossible to determine with certainty whether the omission of a virus characteristic from a description indicates that the virus concerned lacks that attribute (thus requiring a value of 'False' for the associated variable), or whether the attribute was either not sought or impossible to evaluate (requiring a value of 'Indeterminate' for the variable). In this study, the absence of explicit information about a characteristic has been construed as absence of the feature.

The MONA algorithm employed by **Kaufman et al (1990, p. 298)** also assumes that there are no missing values for the variables used to group the data. As monothetic analysis deals with binary variables, the variables used in this study to store the information for analysis are Boolean variables, which may have a value of either 'True' or 'False'. Missing values in the data, however, require representation of a third value, that of 'Indeterminate'. This means that at least a ternary variable is required, or possibly a variable with more than three values if it is necessary to distinguish between differing categories of 'Indeterminate' values. The incorporation of such features tranfers the variable types from simple binary to multiple-valued types for which polythetic analysis should be used. This feature has not been included in the model used in this research, and the data for analysis has been screened and evaluated to either of the possible binary values permissible for use. In a working model, however, means of dealing with uncertainty of the above types would be required. Another data

characteristic which was found in the ***VSUM*** information was that where a single value was used to indicate possession of several features. An example of this type of value is the 'All' value for 'Type of File Infected'. The use of values implying universality is short sighted, as (in this case) new file types have occurred regularly during recent years. For example, does such a value imply executable files with extensions of .COM and .EXE only are under threat, or should .OVL files be included as well? Are file formats used within Microsoft's 'Windows' environment also vulnerable?

The use of this type of variable value will require considerable effort to resolve when the diversity of file types reaches an unmanageable level, and until that time will doubtless give rise to problems of interpretation.

Numerous discrepancies were noted when comparing the ***Virus Bulletin*** classifications with the corresponding ***VSUM*** classification. Many of these involved variations which could be deemed insignificant, possibly arising either from natural variation caused by virus propagation, or by divergent classification techniques or human error. One such dissimilarity was the variation in the reported infective length, which frequently varied in the range of 1 - 5 bytes.

Other differences, however, were direct contradictions. It appeared from many of these discrepancies that different variations of the same virus had been given the same name. It is impossible to be certain, in these cases,

whether the two main authorities whose reports were used for this study have, for any such conflict, been classifying the same code. Furthermore, it is possible that the departures have arisen from varying philosophies in the two organisations, as ***Virus Bulletin*** is still heavily committed to virus identification by the use of signatures (fragments of code which are intended to uniquely identify a virus), and consistently publish lists of such signatures with listings of new reported viruses. This requires that whenever an existing virus is changed, it must be recognised as a new variant if the old signature no longer identifies the new code. ***VSUM***, on the other hand, may consider other factors when establishing differentiation criteria, such as functional similarity or common code fragments.

The data in the ***VSUM*** format used in this study is of limited use for genuine research purposes, containing, as it does, many potential ambiguities in content and uncertainty as to the completeness of the data. This does not diminish its suitability for use as test data to evaluate the classification method proposed.

It is essential that for analytical research which requires detailed analysis of the information itself, stored data is used which is both complete and accurate: this may entail custom collection of data.

Monothetic Suitability

A monothetic analysis demonstration program, described by **Kaufman et al (1990, p 280)**, allows the user to specify how many variables of those

available should be used for the analysis. The analysis then uses all variables available and continues to group the data until either all variables have been used, or the data has been grouped until they cannot be further decomposed. This may be when all remaining available variable values cannot produce a further split, or a when group consists of a single object.

The method described is suitable for use in grouping data on computer virus characteristics. The data, however, must be both complete and accurate. Some doubt existed about the data used for the current study for both completeness and accuracy. The accumulation of data suitable for more detailed study will require a standardised collection and evaluation regime.

The method used in this study is slightly different. A depth-mediated approach has been used where the number of levels in the binary 'tree' showing the split paths is determined by values in the database. The analysis is then free to proceed to the specified depth, using the variables with the strongest association from those specified for use.

Several techniques are available for the grouping of binary data, some of which are monothetic (using one essential item) and others which are polythetic methods. The monothetic approach used in this study follows the method suggested by **Kaufman et al (1990, p.280)** in their MONA algorithm, developed from an earlier method attributed by **Kaufman et al**

(1990, p.304), to the 1959 work of Williams and Lambert, who termed the method 'Associative Analysis'.

Modifiability

Some reorganisation was evident when comparing the earlier classifications from **Fites P et al (1992)** and **Levin R (1990)**, to the current ***VSUM*** data of Patricia Hoffman. Several viruses which had in the former, derived, lists been recognised as individual viruses have been recategorised as variants of existing viruses. This type of dynamism justifies the inclusion of flexibility as a design prerequisite for the classification system. Reclassification using the database system developed in this study would require only execution of the analysis program, using the updated data. As the program uses the data to carry out the grouping, no user intervention is necessary as long as the data is complete and represented by binary variables.

Data expansion will be no problem in the system presented, either for volume increase (new virus records to be added) or for characteristic additions (addition of new virus characteristics). Additional records may be easily added for new virus occurrences, and new fields for additional binary variables which were not included in the original database design may equally be added with little effort, to both VIRBIN and NODEVARS.

No modification to the processing program is necessary to accommodate the changes indicated above. This is a slight improvement on the MONO

program described by **Kaufman et al (1990, p.284)**, which requires internal program modifications to array sizes if more than 200 records are to be processed.

However, the problem remains as to how to ensure the completeness of the data. For instance, the promulgation of a new classification variable would require a value for this variable, not only for newly reported viruses, but for all previously recorded viruses. The provision and maintenance of such a body of information is presently challenging, but the current rate of increase will ultimately require some form of automated analysis tool which could carry out a 'virus dissection' and report the results in terms of the required variables.

Currently the depth to which the program will partition is static. However, it is quite easy to increase or decrease the depth by adding or deleting records in NODEVARS database. Making the depth parameter an interactive user choice would be a matter of some minor alterations to the program code.

CHAPTER 5 - CONCLUSIONS

Nomenclature

The question of nomenclature has not been previously discussed in the body of this study. There are several considerations for which no provision is currently made in the naming conventions used. The first matter is the encapsulation, within the name, of the parent virus in respect of virus variants. If it is considered desirable to perpetuate the system of viruses and variants, it is recommended that the current hierarchical recording system where all variant details are stored as detail of the parent virus is abolished. A suggested replacement for the existing method is to create a separate record for each virus, with a 'parent' field included in it. This would facilitate changes to genealogy if necessary with the minimum of fuss, but would also ensure, most importantly, that every virus and variant has its characteristics separately and completely listed for classification. One feasible naming convention for display which is already in use by ***Virus Bulletin*** and commends itself to the author is the use of dot notation so that a variant name would become:

'PARENTNAME . VARIANTNAME'

This form is flexible in that multiple levels of descent may be represented, if necessary, by the addition of further dotted extensions, for instance:

'PARENTNAME . VARIANTNAME . SUBVARIANTNAME'

The method may also be used in combination with the virus generation nomenclature discussed on pages 41 - 42.

A significant question which requires an answer, however, is whether the current system of linking a virus variant to a perceived ancestor is to be continued. The question of virus derivation is open to considerable interpretation and many viruses have been found to contain features of several unrelated precursors. The pattern identification criteria for the variant may be quite different from the parent, as will be the characteristics which distinguish the two viruses. Under these circumstances, it would seem undesirable to perpetuate a system which has questionable merit as it is irrelevant, and is likely to become progressively more so with time.

Another question regarding nomenclature which is related to the parent/variant problem, is that of the naming convention to identify viruses created by virus generation mechanisms. These include virus construction kits, variable encryption engines, and other polymorphic engines which either generate virus code *ab initio*, or assist in virus concealment by altering the appearance of the code. Viruses depending on one such mechanism tend to share certain common attributes, such as particular code fragments which may be reused by a particular generation process, or a common encryption/decryption routine which must be incorporated in the propagated virus code. In such cases, where the derivation of a variant is clearly linked to its progenitor, and in many cases also to its identification criteria, it may be more justifiable to include the parentage in the variant name. For these cases, it is recommended that a notation be adopted which is different from that used for ordinary variants. One possibility would be the

notation 'GENERATORNAME->VARIANTNAME'. Storage of this information would require a database field to accommodate the information.

Classification system

The monothetic method of grouping which has been used in this study is suitable for implementing a classification system, as long as the variables on which the classification is based are entirely binary, or may be reduced to binary variables. One method of achieving this is 'clumping', where one non-binary variable is divided into several binary variables, each covering a certain range of the original variable's values, although the questions of variable strength, analysis bias and processing duration require careful consideration before wide use of this technique, as discussed in Chapter 1, under the section 'Reasons for selection of Analysis Technique used'. If any characteristics possess values which may not be represented as binary variables, one of the polythetic cluster analysis methods should be chosen.

Data collection

Considerable comment has been made about the unsuitability of the data collected for this study for the purpose any serious or extended research.

The ***VSUM*** data is incomplete, the details provided are frequently lacking, the format is not standard and it is frequently not possible to determine whether a virus falls into a particular category or not.

Virus Bulletin provides two categories of report. The bulk reports cover all new virus and variant occurrences as they are received and examined, but contain too little detail to be useful for analysis purposes. The second report type is a full virus analysis, which provide excellent detail, but in textual form, requiring extraction of variable details by reading the full description. These detailed descriptions are also too few to provide significant coverage of the field (two to three per month are published).

The only feasible solution to this problem is to engage in a long term data collection exercise, where the data can be captured and stored in the detail and format which facilitates analysis and be promptly updated with new information as it becomes available. This is a daunting prospect, for which special purpose tools and specially trained personnel would undoubtedly be required.

Determination of virus characteristics for classification would frequently require disassembly and examination of the virus code. This requires that a copy of the virus should be in the possession of the classifier, requiring the establishment and maintenance of a secure library of viral code.

Attainment of Objectives

Reviewing the research objectives and considering the degree to which they have been fulfilled by the completion of this study, it is believed that the main objective of the development of an unambiguous, extensible and modifiable classification system for computer viruses in the IBM PC/DOS environment using binary variables and monothetic analysis has been demonstrably achieved. There are, however, several caveats which should be entered about full implementation of this system, including questions such as:

1. The initial availability of accurate and complete data on which a full classification may be based.
2. Whether all pertinent variables may be adequately represented as binary variables without adversely affecting the classification balance.
3. The update and maintenance of the database with new virus reports and variable information.

The subsidiary objective concerning nomenclature has been addressed, and recommendations made. However, the merit of perpetuating the current nomenclature by including perceived progenitor names in variant names is questionable, and requires further consideration.

The objective concerning resolution of delimitation conflicts is closely related to the nomenclature question. If the current system of patronymic nomenclature and classification is not continued, controversy over

derivation will become irrelevant. However, the classification program developed in this study bases classifications purely on virus characteristics, and the ancestry of a virus is neither considered as a point for classification nor produced as an output of the classification. A virus may belong only to the group with which it shares characteristics, and the classification therefore resolves any dispute about the group into which a virus falls.

The subsidiary objective of providing an encoding method to summarise virus characteristics is achieved in this study by the construction, during monothetic analysis, of a descriptor containing the variable names used in grouping each virus. These names, together with the values that the virus possesses for the variables themselves, are the determinant of the virus' grouping. Although the descriptor is relatively long, it provides a comprehensible, abbreviated means of viewing virus classification grouping.

BIBLIOGRAPHY

Blackwelder, R. E. (1967). ***Taxonomy: A Text and Reference Book***, New York: John Wiley & Sons.

Burger, R. (1988). ***Computer Viruses A High-Tech Disease***, Grand Rapids: Abacus.

Burger, R. (1991). ***Computer Viruses and Data Protection***, Grand Rapids: Abacus.

Caelli, W., Longley, D., & Shain, M. (1991). ***Information Security Handbook***, Basingstoke: Macmillan Publishers Ltd.

Cohen, F. B. (1986). Computer Viruses, ***Dissertation Abstracts International 47/11B***, 4608, University Microfilms International.

Fites, P., Johnston, P., & Kratz, M. (1992). ***The Computer Virus Crisis***, New York: Van Nostrand Rheinhold.

Hruska, J. (1990). ***Computer Viruses and Anti-Virus Warfare,*** Chichester: Ellis Horwood Publishers.

Hoffman, P.M (1992 Oct), ***VSUM - Patricia Hoffman's Virus Information Summary List***, (version 9210), [Computer program/ Hypertext database], Distributor: Patricia M. Hoffman, Santa Clara, CA (Address: 333 Bowers Ave, Suite 130, Santa Clara CA. Zip: 95054).

Kamay, V., & Adams, T. (1992). ***The 1992 Profile of Computer Abuse in Australia,*** Melbourne: Australian Computer Abuse Research Bureau.

Kaufman, L. & Rousseeuw, P.J. (1990). ***Finding Groups in Data: An Introduction to Cluster Analysis,*** New York: John Wiley & Sons.

Levin, R. B. (1990). ***The Computer Virus Handbook***, Berkeley: Osborne Mcgraw-Hill.

McAfee, J. (1992). ***Virus Attack and Protection,*** Paper presented at Virus Solutions Conference, Hyatt Regency Hotel, Perth, 19th February, 1992.

McAfee, J. (1992a). ***Virus Characteristics List V89***, computer text file included with virus SCAN software, McAfee Associates, Santa Clara, California.

Miles, M. B. & Huberman, A. M. (1984), ***Qualitative Data Analysis: A Sourcebook of New Methods,*** Newbury Park: Sage Publications.

Virus Bulletin, July 1991 - August 1993, Abingdon Science Park, Oxon, England.

APPENDIX A - Data used for analysis

NAME	RES	MBR	COM	EXE	OVL	DOS BOOT	FD	CMD	O_W	PSITE	SPAWN	FAT	PART	STLTH	ENCRYPT
1,008	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
1024 PRINT SCREEN	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
1024 SBC	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	Y	Y
1,067	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
1,210	Y	N	N	Y	N	N	N	N	N	Y	N	N	N	N	N
1,226	Y	N	Y	N	N	N	N	N	N	Y	N	N	N	N	Y
1,241	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
1,244	Y	N	Y	Y	N	N	N	N	N	Y	N	N	N	N	N
1,253	Y	N	Y	N	N	N	N	Y	N	Y	N	N	Y	N	N
1,260	N	Y	N	N	N	N	N	N	N	Y	N	N	N	N	Y
1,308	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	Y
1,381	N	N	N	Y	N	N	N	N	N	Y	N	N	N	N	N
1,385	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
1,392	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
1,452	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
1,575	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
1,605	Y	N	Y	Y	N	N	N	N	N	Y	N	N	N	N	N
1,661	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
1,720	Y	N	Y	Y	N	N	N	N	N	Y	N	N	N	N	N
1,835	N	N	N	Y	N	N	N	N	N	Y	N	N	N	N	N
1,840	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	Y
1,963	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
2,153	Y	N	Y	Y	N	N	N	N	N	Y	N	N	N	N	N
2,559	N	N	N	Y	N	N	N	N	N	Y	N	N	N	N	N
2,560	Y	N	Y	Y	N	N	N	N	N	Y	N	N	N	N	N
2,623	Y	N	N	Y	N	N	N	N	N	Y	N	N	N	N	N
337	Y	N	Y	N	N	N	N	N	N	Y	N	N	N	N	N
3,445	Y	N	Y	Y	N	N	N	N	N	Y	N	N	N	Y	N
382	N	N	Y	Y	N	N	N	Y	Y	N	N	N	N	N	N
405	N	N	Y	N	N	N	N	N	Y	N	N	N	N	N	N
408	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
4,096	Y	N	Y	Y	Y	N	N	N	N	Y	N	N	N	Y	N
439	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
4,870	N	N	Y	Y	N	N	N	Y	Y	N	N	N	N	N	N
500	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
512	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
5,120	N	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
557	Y	N	N	Y	N	N	N	N	N	Y	N	N	N	N	N
572	Y	N	N	Y	N	N	N	N	N	Y	N	N	N	N	N
595	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
621	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
646	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N

NAME	RES	MBR	COM	EXE	OVL	DOS BOOT	FD	CMD	O_W	PSITE	SPAWN	FAT	PART	STLTH	ENCRYPT
66A	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
7,808	N	N	Y	Y	N	N	N	N	N	Y	N	N	N	N	N
834	Y	N	Y	N	N	N	N	N	N	Y	N	N	N	N	N
914	Y	N	Y	N	N	N	N	N	N	Y	N	N	N	N	N
923	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
981	Y	N	Y	Y	N	N	N	N	N	Y	N	N	N	N	N
ACID	N	N	Y	Y	N	N	N	Y	Y	N	N	N	N	N	N
ADA	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
ADOLPH	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
AFRICAN 109	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
AGENA	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
AH	Y	N	Y	N	N	N	N	N	N	Y	N	N	N	N	N
AIDS	N	N	Y	Y	N	N	N	N	Y	N	N	N	N	N	N
AIDS II	N	N	Y	Y	N	N	N	N	N	N	Y	N	N	N	N
AIRCOP	Y	N	N	N	Y	N	N	N	N	N	N	N	N	N	N
AKUKU	N	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
ALABAMA	Y	N	N	Y	N	N	N	N	N	Y	N	N	N	N	N
ALAMEDA	Y	N	N	N	N	N	Y	N	N	N	N	N	N	N	N
ALBANIA	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
ALEXANDER	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
ALFA	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
ALL SYS 9	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
AMBULANCE CAR	N	N	Y	N	N	N	N	N	N	Y	N	N	N	N	N
AMSTRAD	N	N	Y	N	N	N	N	N	N	Y	N	N	N	N	N
ANDRE	Y	N	Y	Y	N	N	N	N	N	Y	N	N	N	Y	Y
ANIMUS	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
ANT	N	N	Y	N	N	N	N	N	N	Y	N	N	N	N	N
ANTHRAX	Y	N	Y	Y	N	N	N	Y	N	N	N	N	Y	N	N
ANTI-D	Y	N	Y	N	N	N	N	N	N	Y	N	N	N	N	N
ANTI-PASCAL	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
ANTI-PASCAL II	N	N	Y	N	N	N	N	Y	N	N	N	N	N	N	N
ANTI-TEL	Y	Y	N	N	N	N	Y	N	N	N	N	N	Y	Y	N
ANTIMON	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
ANTO	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
ARAGON	Y	Y	N	N	N	Y	Y	N	N	N	N	N	Y	Y	N
ARF	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
ARGENTINA	Y	N	Y	N	N	N	N	N	N	Y	N	N	N	N	N
ARKANOID	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
ARMAGEDDON	Y	N	Y	N	N	N	N	N	N	Y	N	N	N	N	N
ASH	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
ASHAR	Y	N	N	N	N	Y	N	N	N	N	N	N	N	N	N
ASP-472	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
ASTRA	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
AT144	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
ATAS	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
ATHENS	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	Y	N
ATTACK	Y	N	Y	N	N	N	N	N	N	Y	N	N	N	N	N
ATTENTION!	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
AUGUST 16TH	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
AUSTRALIAN	Y	N	Y	Y	N	N	N	N	N	Y	N	N	N	N	N

NAME	RES	MBR	COM	EXE	OVL	DOS BOOT	FD	CMD	O_W	PSITE	SPAWN	FAT	PART	STLTH	ENCRYPT
AUSTRALIAN 403	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
AZUSA	Y	Y	N	N	N	Y	Y	N	N	N	N	N	Y	N	N
BACKTIME	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
BAD BOY	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
BAD BRAIN	N	N	Y	N	N	N	N	Y	Y	N	N	N	N	N	N
BADSEC	Y	N	N	Y	N	N	N	N	N	Y	N	N	N	N	N
BANANA	N	N	Y	N	N	N	N	Y	Y	N	N	N	N	N	N
BANDIT	N	N	N	Y	N	N	N	N	N	Y	N	N	N	N	N
BAOBAB	Y	N	N	Y	N	N	N	N	N	Y	N	N	N	N	N
BARCELONA	Y	N	Y	N	N	N	N	N	N	Y	N	N	N	N	N
BEAST-N-BLACK	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
BEBE	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
BEST WISHES	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
BETA	N	N	Y	N	N	N	N	N	N	Y	N	N	N	N	N
BEWARE	N	N	Y	N	N	N	N	N	N	Y	N	N	N	N	N
BFD	Y	N	N	Y	N	Y	Y	N	Y	N	N	N	N	Y	N
BIG JOKE	N	N	Y	N	N	N	N	N	N	Y	N	N	N	N	N
BLACK MONDAY	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
BLACK WIZARD	N	N	N	Y	N	N	N	N	N	Y	N	N	N	N	N
BLAZE	Y	N	Y	Y	N	N	N	Y	Y	N	N	N	N	N	N
BLINKER	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
BLJEC	N	N	Y	N	N	N	N	N	N	Y	N	N	N	N	N
BLOOD	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
BLOOD LUST	N	N	Y	N	N	N	N	Y	Y	N	N	N	N	N	N
BLOODY!	Y	N	N	N	N	Y	N	N	N	N	N	N	Y	N	N
BOB	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
BOMBER	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
BOOJUM	Y	N	N	Y	N	N	N	N	N	Y	N	N	N	N	N
BOOT KILLER	N	Y	N	N	N	N	N	N	N	N	N	N	Y	N	N
BOW	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
BOYS	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
BRAIN	Y	N	N	N	N	Y	N	N	N	N	N	N	N	N	N
BRAINY	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
BRAZILIAN BUG	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
BURGER	N	N	Y	Y	N	N	N	Y	Y	N	N	N	N	N	N
BURGHOFER	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
BUSTED	N	N	N	Y	N	N	N	N	Y	N	N	N	N	N	N
CADKILL	N	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
CANNABIS	Y	N	N	N	N	Y	Y	N	N	N	N	N	N	N	N
CANSU	Y	Y	N	N	N	Y	Y	N	N	N	N	N	Y	N	N
CAPITALL	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
CARA	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
CARFIELD	Y	N	Y	Y	N	N	N	N	N	Y	N	N	N	N	N
CARIOCA	Y	N	Y	N	N	N	N	N	N	Y	N	N	N	N	N
CASCADE	Y	N	Y	N	N	N	N	N	N	Y	N	N	N	N	N
CASINO	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	Y	N
CASPER	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
CATMAN	Y	Y	N	N	N	Y	Y	N	N	N	N	N	Y	N	N
CAZ	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
CB-1530	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N

NAME	RES	MBR	COM	EXE	OVL	DOS BOOT	FD	CMD	O_W	PSITE	SPAWN	FAT	PART	STLTH	ENCRYPT
CD	Y	N	Y	Y	N	N	N	N	N	Y	N	N	N	N	N
CERBURUS	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
CHAD	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
CHANG	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
CHANGU MANGU	Y	Y	N	N	N	Y	Y	N	N	N	N	N	Y	N	N
CHAOS	Y	N	N	N	N	Y	N	N	N	N	N	N	N	N	N
CHASER	N	N	N	Y	N	N	N	N	N	Y	N	N	N	N	N
CHECKSUM	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
CHEEBA	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	Y
CHEMMY	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
CHRISTMAS IN JAPAN	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
CHRISTMAS TREE	N	N	Y	N	N	N	N	N	N	N	N	N	Y	N	Y
CINDERELLA	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
CLONEWAR	N	N	N	N	N	N	N	N	N	N	Y	N	N	N	N
CLOSE	Y	N	N	Y	N	N	N	N	N	Y	N	N	N	N	N
CMDR BOMBER	Y	N	Y	N	N	N	N	N	N	Y	N	N	N	N	N
COFFESHOP-1568	Y	N	Y	Y	N	N	N	N	N	Y	N	N	N	N	N
COPYRIGHT	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
COSSIGA	N	N	N	Y	N	N	N	N	N	Y	N	N	N	N	N
CRACKER JACK	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
CRASH	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
CRAZY EDDIE	Y	Y	Y	Y	N	N	N	Y	N	N	N	N	Y	N	N
CRAZY IMP	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	Y	N
CREEPER	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
CREW-2480	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
CRF	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
CRIMINAL	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
CSL	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
CURSE BOOT	Y	Y	N	N	N	Y	Y	N	N	N	N	N	N	Y	N
CV4	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
CYBER	N	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
DAD	Y	N	Y	N	N	N	N	N	N	Y	N	N	N	N	N
DADA	Y	N	N	Y	N	N	N	N	N	Y	N	N	N	N	N
DAMAGE	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
DAME (DARK AVENGER MUT MACH)	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
DARK AVENGER	Y	N	Y	Y	Y	N	N	Y	N	Y	N	N	N	N	N
DARK LORD	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
DARTH VADER	Y	N	Y	N	N	N	N	Y	Y	N	N	N	N	N	N
DATACRIME	N	N	Y	N	N	N	N	N	N	Y	N	N	N	N	Y
DATALOCK	Y	N	N	Y	N	N	N	Y	N	Y	N	N	N	N	N
DAVIS	Y	N	N	Y	N	N	N	N	N	Y	N	N	N	N	N
DAY10	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
DBASE	Y	N	Y	N	Y	N	N	N	N	Y	N	N	N	N	N
DEFINE	N	N	Y	Y	N	N	N	Y	Y	N	N	N	N	N	N
DEICIDE	N	N	Y	N	N	N	N	N	Y	N	N	N	N	N	N
DEMOLITION	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
DEN ZUK	Y	N	N	N	N	N	Y	N	N	N	N	N	N	N	N
DEST	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N

NAME	RES	MBR	COM	EXE	OVL	DOS BOOT	FD	CMD	O_W	PSITE	SPAWN	FAT	PART	STLTH	ENCRYPT
DESTRUCTOR V4.0	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
DEVIL'S DANCE	Y	N	Y	N	N	N	N	N	N	Y	N	Y	N	N	N
DEWDZ	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
DIMA	N	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
DIR VIRUS	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
DIR-2	Y	N	Y	Y	N	N	N	Y	N	N	N	N	N	Y	N
DISCOM	Y	N	Y	Y	N	N	N	N	N	Y	N	N	N	N	N
DISK KILLER	Y	N	N	N	N	Y	N	N	N	N	N	Y	N	N	N
DM	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
DO-NOTHING	Y	N	Y	N	N	N	N	N	N	Y	N	N	N	N	N
DODO	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
DOOM II	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
DOT KILLER	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
DUTCH 555	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
DUTCH TINY	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
EAR	N	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
EDEL	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	Y	N
EDV	Y	Y	N	N	N	Y	N	N	N	N	N	N	Y	N	N
EIGHT TUNES	Y	N	Y	Y	Y	N	N	N	N	Y	N	N	N	N	N
EINSTEIN	Y	N	N	Y	N	N	N	N	N	Y	N	N	N	N	N
ELIZA	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
EMF	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
EMMIE	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	Y	N
END OF	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
ENEMY	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	Y
ENIGMA	N	N	N	Y	N	N	N	N	N	Y	N	N	N	N	N
ENOLA	Y	N	Y	Y	N	N	N	N	N	Y	N	N	N	N	N
ERROR	Y	N	N	Y	N	N	N	N	N	Y	N	N	N	N	N
ETC	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
EUROPE-92	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
EVIL	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	Y
EVIL EMPIRE	Y	Y	N	N	N	Y	Y	N	N	N	N	N	Y	N	N
EXEBUG	Y	Y	N	N	N	Y	Y	N	N	N	N	N	Y	N	N
EXPLODE	N	N	Y	N	N	N	N	Y	Y	N	N	N	N	N	N
EXUNT	N	N	Y	N	N	N	N	N	N	Y	N	N	N	N	N
FATHER	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
FATHER CHRISTMAS	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
FATHER XMAS	N	N	Y	N	N	N	N	Y	N	N	N	N	N	N	N
FCB	N	N	Y	Y	N	N	N	Y	Y	N	N	N	N	N	N
FEIST	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
FELLOWSHIP	Y	N	N	Y	N	N	N	N	N	Y	N	N	N	N	N
FGT	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
FICH	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
FICHV-896	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
FIL	Y	N	Y	N	Y	N	N	Y	N	Y	N	N	N	N	N
FILLER	Y	Y	N	N	N	Y	Y	N	N	N	N	N	Y	Y	N
FINGERS	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
FINNISH-709	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
FISH	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	Y
FISH BOOT	Y	Y	N	N	N	Y	Y	N	N	N	N	N	Y	N	N

NAME	RES	MBR	COM	EXE	OVL	DOS BOOT	FD	CMD	O_W	PSITE	SPAWN	FAT	PART	STLTH	ENCR YPT
FLASH	Y	N	Y	Y	N	N	N	N	N	Y	N	N	N	N	N
FLIP	Y	Y	Y	Y	Y	N	N	Y	N	Y	N	N	Y	N	N
FLOWER	N	N	N	Y	N	N	N	N	N	Y	N	N	N	N	N
FORGER	Y	N	N	Y	N	N	N	N	N	Y	N	N	N	N	Y
FORM	Y	Y	N	N	N	Y	N	N	N	N	N	N	N	N	N
FREEW-692	N	N	Y	N	N	N	N	N	N	Y	N	N	N	N	N
FRERE JACQUES	Y	N	Y	Y	Y	N	N	N	N	Y	N	N	N	N	N
FRIDAY 13TH COM	N	N	Y	N	N	N	N	N	N	Y	N	N	N	N	N
FRIENDS	Y	N	N	Y	N	N	N	N	N	Y	N	N	N	N	N
FRODO SOFT	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
FROGS	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
FU MANCHU	Y	N	Y	Y	Y	N	N	N	N	Y	N	N	N	N	Y
FUNERAL	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
FUNGUS	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
GEEK	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
GERGANA	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
GHOSTBALLS	N	N	Y	N	N	Y	N	N	N	Y	N	N	N	N	N
GLISS	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
GLOBE	N	N	N	Y	N	N	N	N	N	N	Y	N	N	N	N
GNOSE	Y	N	Y	Y	N	N	N	Y	N	Y	Y	N	N	N	Y
GOSIA	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
GOT-YOU	N	N	N	Y	N	N	N	N	N	Y	N	N	N	Y	N
GOTCHA	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
GRAPJE	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
GREEN JOKER	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
GREEN PEACE	N	N	N	Y	N	N	N	N	Y	N	N	N	N	N	N
GREMLIN	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
GRITHER	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
GROEN LINKS	Y	N	Y	Y	N	N	N	N	N	Y	N	N	N	N	N
GROOVE	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	Y
GROWING BLOCK	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
GRUNT-1	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
GUILLON	Y	Y	N	N	N	Y	Y	N	N	N	N	N	Y	N	N
GUPPY	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
HA	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
HACKTIC	N	N	N	Y	N	N	N	N	Y	N	N	N	N	N	N
HAFENSTRASS	N	N	N	Y	N	N	N	N	N	Y	N	N	N	N	N
HAIFA	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	Y
HALLOECHEN	Y	N	Y	Y	N	N	N	N	N	Y	N	N	N	N	N
HALLOWEEN	N	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
HAPPY	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
HAPPY NEW YEAR	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
HARAKIRI	N	N	Y	Y	N	N	N	Y	Y	N	N	N	N	N	N
HARY ANTO	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	Y
HASTINGS	N	N	Y	N	N	N	N	Y	Y	N	N	N	N	N	N
HELL	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
HELLRAISER	N	N	N	Y	N	N	N	N	Y	N	N	N	N	N	N
HELLWEEN	Y	N	Y	Y	N	N	N	N	N	Y	N	N	N	N	N
HERO	Y	N	Y	Y	N	N	N	N	N	Y	N	N	N	N	N
HERO-394	Y	N	N	Y	N	N	N	N	N	Y	N	N	N	N	N

NAME	RES	MBR	COM	EXE	OVL	DOS BOOT	FD	CMD	O_W	PSITE	SPAWN	FAT	PART	STLTH	ENCR YPT
HH&H	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
HI	Y	N	N	Y	N	N	N	N	N	Y	N	N	N	N	N
HIGHLANDER	Y	N	Y	N	N	N	N	N	N	Y	N	N	N	N	N
HITCHCOCK	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
HOLOCAUST	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	Y	Y
HOMINY	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
HORROR	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
HORSE BOOT	Y	Y	N	N	N	Y	Y	N	N	N	N	N	Y	N	N
HUNGARIAN	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
HUNGARIAN 482	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
HYBRYD	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
HYDRA FAMILY	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
HYMN	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
I-B	N	N	Y	N	N	N	N	N	Y	Y	N	N	N	N	N
ICE 9	Y	N	Y	N	N	N	N	N	N	Y	N	N	N	N	N
ICELANDIC	Y	N	N	Y	N	N	N	N	N	Y	N	N	N	N	N
IDLE	Y	N	Y	Y	N	N	N	N	N	Y	N	N	N	N	N
IKV 528	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
ILL	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
INCOM	N	N	Y	N	N	N	N	N	N	Y	N	N	N	N	N
INFINITY	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
INTERCEPTOR	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
INTRUDER	N	N	N	Y	N	N	N	N	N	Y	N	N	N	N	N
INVADER	Y	N	Y	Y	N	Y	N	N	N	Y	N	N	N	N	N
INVOL	Y	N	N	Y	N	N	N	N	N	Y	N	N	N	N	N
IRAQUI WARRIOR	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
IT	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
ITALIAN 803	N	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
ITAVIR	N	N	N	Y	N	N	N	N	N	Y	N	N	N	N	N
ITTI	N	N	Y	N	N	N	N	Y	Y	N	N	N	N	N	N
JD	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
JEFF	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
JERK	N	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
JERUSALEM	Y	N	Y	Y	N	N	N	N	N	Y	N	N	N	N	N
JERUSALEM 11-30	Y	N	Y	Y	N	N	N	N	N	Y	N	N	N	N	N
JERUSALEM 1767	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
JOANNA	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
JOJO	Y	N	Y	N	N	N	N	N	N	Y	N	N	N	N	N
JOJO 2	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
JOKER	N	N	N	Y	N	N	N	N	N	Y	N	N	N	N	N
JOKER 2	Y	N	Y	Y	N	N	N	N	N	Y	N	N	N	N	N
JOSHI	Y	Y	N	N	N	Y	N	N	N	N	N	N	Y	N	N
JULY 13TH	N	N	N	Y	N	N	N	N	N	Y	N	N	N	N	N
JULY 26TH	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
JUNE 16TH	N	N	Y	N	N	N	N	N	N	Y	N	N	N	N	N
JW2	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
KALAH	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
KAMIKAZI	N	N	N	Y	N	N	N	N	Y	N	N	N	N	N	N
KARIN	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
KEMEROVO	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N

NAME	RES	MBR	COM	EXE	OVL	DOS BOOT	FD	CMD	O_W	PSITE	SPAWN	FAT	PART	STLTH	ENCRYPT
KEYBOARD BUG	Y	N	Y	Y	N	N	N	N	N	Y	N	N	N	N	N
KEYDROP	Y	Y	N	N	N	Y	Y	N	N	N	N	N	N	N	N
KEYPRESS	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
KIEV 483	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
KIT	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
KLAEREN	Y	N	Y	Y	N	N	N	N	N	Y	N	N	N	N	N
KODE4	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
KOREA	Y	N	N	N	N	Y	Y	N	N	N	N	N	N	N	N
KRIVMOUS	N	N	Y	Y	N	N	N	N	N	Y	N	N	N	N	N
KUKU-448	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
LABEL	Y	N	Y	N	N	N	N	Y	Y	N	N	N	N	N	N
LANCS	N	N	N	Y	N	N	N	N	N	N	Y	N	N	N	N
LAZY	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
LEECH	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
LEGALIZE	Y	N	Y	Y	N	N	N	N	N	Y	N	N	N	N	N
LEHIGH	Y	N	N	N	N	N	N	Y	Y	N	N	Y	N	N	N
LEPROSY	N	N	Y	Y	N	N	N	Y	Y	N	N	N	N	N	N
LIBERTY	Y	N	Y	Y	Y	N	N	Y	N	Y	N	N	N	N	Y
LIBERTY-1172	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
LIBERTY-2	Y	Y	Y	Y	Y	N	N	Y	N	Y	N	N	N	N	Y
LISBON	N	N	Y	N	N	N	N	N	N	Y	N	N	N	N	N
LITTLE BROTHER	Y	N	Y	Y	N	N	N	N	N	N	Y	N	N	N	N
LITTLE GIRL	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
LITTLE PIECES	Y	N	N	Y	N	N	N	N	N	Y	N	N	N	N	N
LOA DUONG	Y	Y	N	N	N	Y	Y	N	N	N	N	N	N	N	N
LOCKUP	Y	N	Y	Y	N	N	N	N	N	N	Y	N	N	N	N
LOWERCASE	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
LOZINSKY	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
LUCIFER	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
LYCEE	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
LZ	N	N	Y	Y	N	N	N	N	N	N	Y	N	N	N	N
M.I.R.	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
MACEDONIA	Y	N	Y	N	N	N	N	N	N	Y	N	N	N	N	N
MADISMO	N	N	N	Y	N	N	N	N	Y	N	N	N	N	N	N
MAGNITOGORSK 2048	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	Y	N
MALAGA	Y	Y	Y	Y	N	Y	Y	N	N	Y	N	N	N	Y	N
MALAISE	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
MALMSEY	N	N	Y	N	N	N	N	Y	Y	N	N	N	N	N	N
MALTESE AMOEBA	Y	N	Y	Y	N	N	N	N	N	Y	N	N	N	N	N
MANNEQUIN	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
MANOLA	Y	N	Y	N	N	N	N	N	N	Y	N	N	N	N	N
MANTA	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
MARAUDER	N	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
MARDI BROS	Y	N	N	N	N	Y	Y	N	N	N	N	N	N	N	N
MARL	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
MAX	Y	Y	N	N	N	Y	Y	N	N	N	N	N	Y	N	N
MAYAK	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	Y	N
MEDICAL	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
MEXICAN MUD	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N

NAME	RES	MBR	COM	EXE	OVL	DOS BOOT	FD	CMD	O_W	PSITE	SPAWN	FAT	PART	STLTH	ENCRYPT
MG	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
MGTU	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
MICHELANGELO	Y	Y	N	N	N	Y	Y	N	N	N	N	N	Y	N	N
MICRO 128	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
MICROBES	Y	N	N	N	N	Y	N	N	N	N	N	N	N	N	N
MICROPOX	Y	N	Y	Y	N	N	N	N	N	Y	N	N	N	N	N
MIKY	Y	N	Y	Y	N	N	N	N	N	Y	N	N	N	N	N
MILENA	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
MINI-45	N	N	Y	N	N	N	N	Y	Y	N	N	N	N	N	N
MINISTRY	N	N	Y	N	N	N	N	N	N	Y	N	N	N	N	N
MINSK GHOST	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	Y	N
MIRROR	Y	N	N	Y	N	N	N	N	N	Y	N	N	N	N	N
MIX1	Y	N	N	Y	N	N	N	N	N	Y	N	N	N	N	N
MIX2	Y	N	Y	Y	N	N	N	N	N	Y	N	N	N	N	N
MOCTEZUMA'S REVENGE	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
MONO	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
MONTH 4-6	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
MONXLA	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
MONXLA B	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
MOSQUITO	Y	N	N	Y	N	N	N	N	N	Y	N	N	N	N	N
MPS 1.1	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
MPS 3.1	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
MPS 3.2	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
MPS 4.01	Y	N	N	Y	N	N	N	N	N	Y	N	N	N	N	N
MSHARK	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
MSTU	N	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
MUGSHOT	Y	N	N	N	N	Y	Y	N	N	N	N	N	N	N	N
MULE	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
MULTI-123	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
MULTI-FACE	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
MUMMY	Y	N	N	Y	N	N	N	N	N	Y	N	N	N	N	N
MUNICH	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
MURPHY	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
MUSICBUG	Y	Y	N	N	N	Y	N	N	N	N	N	N	Y	N	N
MUTANT FAMILY	N	N	Y	N	N	N	N	Y	Y	Y	N	N	N	N	N
NAUGHTY HACKER	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	Y	N
NEWCOM	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
NINA	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
NINES	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
NO FRILLS	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
NOBOCK	N	N	Y	N	N	N	N	N	N	Y	N	N	N	N	N
NOINT	Y	Y	N	N	N	Y	Y	N	N	N	N	N	Y	N	N
NOMENKLATURA	Y	N	Y	Y	N	N	N	Y	N	N	N	N	N	N	N
NOVEMBER 17TH	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
NOWHERE MAN	N	N	Y	Y	N	N	N	Y	Y	N	N	N	N	N	N
NPOX	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	Y	N
NTKC	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
NULL SET	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
NULL-178	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N

NAME	RES	MBR	COM	EXE	OVL	DOS BOOT	FB	CMD	O_W	PSITE	SPAWN	FAT	PART	STLTH	ENCRYPT
NUMBER ONE	N	N	Y	N	N	N	N	N	Y	N	N	N	N	N	N
NYGUS	Y	N	Y	Y	N	N	N	N	N	Y	N	N	N	N	N
OHIO	Y	N	N	N	N	Y	Y	N	N	N	N	N	N	N	N
OMT	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
ONDRA	N	N	N	Y	N	N	N	N	Y	N	N	N	N	N	N
ONTARIO	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
ONTARIO III	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	Y	N
ONTARIO-730	Y	N	Y	Y	Y	N	N	N	N	Y	N	N	N	N	N
OROPAX	Y	N	Y	N	N	N	N	N	N	Y	N	N	N	N	N
OTTO6	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	Y
PA	N	N	N	Y	N	N	N	N	N	Y	N	N	N	N	N
PADDED	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
PARASITE	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
PARIS	N	N	Y	Y	Y	N	N	Y	N	Y	N	N	N	N	N
PARITY	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
PARTICLE MAN	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
PASCAL-4260	N	N	Y	Y	N	N	N	N	Y	N	N	N	N	N	N
PASCAL-5220	N	N	Y	Y	N	N	N	Y	Y	N	N	N	N	N	N
PATH	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
PATHHUNT	N	N	Y	Y	N	N	N	N	N	Y	N	N	N	N	N
PATIENT	Y	N	Y	Y	N	N	N	N	N	Y	N	N	N	N	Y
PC FLU	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
PC FLU-2	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
PCBB	Y	N	N	N	N	N	N	Y	N	Y	N	N	N	N	N
PCV	Y	N	Y	Y	N	N	N	N	N	Y	N	N	N	N	N
PENTAGON	Y	N	N	N	N	N	Y	N	N	N	N	N	N	N	Y
PENZA	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
PERFUME	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
PHANTOM	Y	N	Y	N	N	N	N	N	N	Y	N	N	N	N	N
PHOENIX	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
PHOENIX 2000	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
PHOENIXD	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
PI	Y	N	N	Y	N	N	N	N	N	Y	N	N	N	N	N
PIAZOLLA	Y	N	Y	N	N	N	N	N	N	Y	N	N	N	N	N
PIF	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
PILA	Y	N	Y	Y	N	N	N	N	N	Y	N	N	N	N	N
PINGPONG	Y	N	N	N	N	Y	Y	N	N	N	N	N	N	N	N
PIRATE	N	N	Y	N	N	N	N	Y	Y	N	N	N	N	N	N
PISELLO	Y	N	N	Y	N	N	N	N	N	Y	N	N	N	N	N
PITCH	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
PIXEL	N	N	Y	N	N	N	N	N	N	Y	N	N	N	N	N
PIXIE	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
PLASTIQUE	Y	N	Y	Y	N	N	N	N	N	Y	N	N	N	N	N
PLASTIQUE-B	Y	N	Y	Y	N	Y	Y	N	N	N	N	N	N	N	N
PLOVDIV 1.1	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
PLOVDIV 1.3	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
PLUTTO	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
POEM	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
POGUE	Y	N	Y	N	N	N	N	N	N	Y	N	N	N	N	Y
POJER	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N

NAME	RES	MBR	COM	EXE	OVL	DOS BOOT	FD	CMD	O_W	PSITE	SPAWN	FAT	PART	STLTH	ENCRYPT
POLIMER	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
POLISH 217	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
POLISH 529	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
POLISH 583	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
POLISH-376	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
POLISH-45	N	N	Y	N	N	N	N	Y	Y	N	N	N	N	N	N
POSSESSED	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
POSSUM	N	N	Y	N	N	N	N	Y	Y	N	N	N	N	N	N
PREGNANT	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
PRIME	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
PRINT SCREEN	Y	Y	N	N	N	Y	N	N	N	N	N	N	N	N	N
PROBLEM	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
PROTECTO	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
PROUD	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
PS-MPC	N	N	Y	Y	N	N	N	Y	Y	Y	N	N	N	N	N
PSYCHOGENIUS	N	N	Y	Y	N	N	N	Y	Y	N	N	N	N	N	N
QMU	Y	Y	Y	N	N	N	N	Y	N	N	N	N	Y	N	N
QP3	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
QUAKE	Y	N	N	Y	N	N	N	N	N	Y	N	N	N	N	N
QUEENS	Y	Y	N	N	N	Y	Y	N	N	N	N	N	Y	N	N
QUIET	Y	N	Y	N	N	N	N	N	N	Y	N	N	N	N	N
QUIRK	N	N	N	Y	N	N	N	N	N	N	Y	N	N	N	N
R-10	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
R-11	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
RAGE	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
RAM VIRUS	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
RATTLE	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
RAUBKOPIE	N	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
REBOOT	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
RED DIAVOLYATA	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
REKLAMA	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
RELZFU	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
RESET	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
RETURNS	Y	N	N	Y	N	N	N	N	N	Y	N	N	N	N	N
REVENGE ATTACKER	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
RNA	N	N	Y	Y	N	N	N	N	N	Y	N	N	N	N	N
ROCKO	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	Y	N
ROSEN	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
RPVS	N	N	Y	N	N	N	N	N	N	Y	N	N	N	N	N
RSP-1876	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
RYBKA	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
SAD	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
SADDAM	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
SADIST	N	N	N	Y	N	N	N	N	N	Y	N	N	N	N	N
SATURDAY THE 14TH	Y	N	Y	Y	Y	N	N	N	N	Y	N	N	N	N	N
SCOTT'S VALLEY	Y	N	Y	Y	N	N	N	N	N	Y	N	N	N	N	N
SCREAM	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
SELF	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N

NAME	RES	MBR	COM	EXE	OVL	DOS BOOT	FD	CMD	O_W	PSITE	SPAWN	FAT	PART	STLTH	ENCRYPT
SEMTEX	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
SENTINEL	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
SEVENTH SON	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
SHADOW	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
SHAKE	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
SHAKER	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
SHHS	N	N	Y	Y	N	N	N	Y	Y	N	N	N	N	N	N
SHIELD	Y	N	Y	Y	N	N	N	N	N	Y	Y	N	N	N	N
SICILIAN MOB	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
SILENCE	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
SILLY	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
SILLY WILLY	N	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
SILLY-365	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
SILVER DOLLAR	N	N	Y	Y	N	N	N	Y	Y	N	N	N	N	N	N
SIMULATI	N	N	Y	N	N	N	N	N	N	Y	N	N	N	N	N
SISKIN	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
SISTOR	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
SKISM 1992	N	N	N	Y	N	N	N	N	Y	N	N	N	N	N	N
SLAYER FAMILY	N	N	Y	Y	N	N	N	N	N	Y	N	N	N	N	N
SLOVAK	N	N	N	Y	N	N	N	N	N	Y	N	N	N	N	N
SLOW	Y	N	Y	Y	Y	N	N	N	N	Y	N	N	N	N	N
SMALL-38	N	N	Y	Y	N	N	N	Y	Y	N	N	N	N	N	N
SMILEY	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
SOLANO 2000	Y	N	Y	N	N	N	N	N	N	Y	N	N	N	N	N
SOMETHING	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
SORRY	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
SOV	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
SPANISH	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
SPANISH APRIL FOOLS	Y	N	N	Y	N	N	N	N	N	Y	N	N	N	N	N
SPANZ	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
SPARSE	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
SPYER	Y	N	Y	Y	N	N	N	N	N	Y	N	N	N	N	N
SQUAWK	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
SQUEAKER	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
SQUISHER	Y	N	Y	N	N	N	N	Y	Y	N	N	N	N	Y	N
STAF	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
STAHL	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
STANCO	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
STARDOT 600	N	N	N	Y	N	N	N	N	N	Y	N	N	N	N	N
STARDOT 789	N	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
STARDOT 801	N	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
STICKY	Y	Y	Y	Y	Y	N	N	Y	N	Y	N	N	Y	N	Y
STINKFOOT	N	N	Y	N	N	N	N	N	N	Y	N	N	N	N	N
STONE '90	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
STONED	Y	Y	N	N	N	N	N	N	N	N	N	N	Y	N	N
STRIKER #1	N	N	Y	N	N	N	N	N	N	Y	N	N	N	N	N
STUPID-1355	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
SUNDAY	Y	N	Y	Y	Y	N	N	N	N	N	N	Y	N	N	N
SUNDAY-2	Y	N	Y	Y	Y	N	N	Y	N	Y	N	N	N	N	N

NAME	RES	MBR	COM	EXE	OVL	DOS BOOT	FD	CMD	O_W	PSITE	SPAWN	FAT	PART	STLTH	ENCRYPT
SURIV 1.01	Y	N	Y	N	N	N	N	N	N	N	N	N	N	N	N
SURIV 2.01	Y	N	N	Y	N	N	N	N	N	Y	N	N	N	N	N
SURIV 3.00	Y	N	Y	Y	Y	N	N	N	N	Y	N	N	N	N	N
SURRENDER	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
SVC 3.1	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
SVC 4.0	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
SVC 5.0	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	Y	N
SVC 6.0	Y	Y	Y	Y	N	N	N	N	N	Y	N	N	Y	N	N
SVERDLOV	Y	N	Y	Y	Y	N	N	Y	N	N	N	N	N	N	Y
SVIR	N	N	N	Y	N	N	N	N	N	Y	N	N	N	N	N
SWAP	Y	N	N	N	N	N	Y	N	N	N	N	N	N	N	N
SWEDISH BOYS	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
SWEDISH DISASTER	Y	Y	N	N	N	Y	Y	N	N	N	N	N	Y	N	N
SWISS 143	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
SWISS PHOENIX	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	Y	N
SYLVIA	Y	N	Y	N	N	N	N	N	N	Y	N	N	N	N	N
SYSLOCK	N	N	Y	Y	N	N	N	N	N	Y	N	N	N	N	N
TABULERO	Y	N	N	Y	N	N	N	N	N	Y	N	N	N	N	N
TACK	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
TAIWAN	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
TAIWAN 3	Y	N	Y	Y	Y	N	N	N	N	Y	N	N	N	N	N
TAIWAN 4	Y	N	Y	Y	N	N	N	N	N	Y	N	N	N	N	N
TALENTLESS	N	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
TELECOM	Y	N	Y	N	N	N	N	N	N	Y	N	N	N	N	Y
TENBYTES	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
TEQUILA	Y	Y	N	Y	N	N	N	N	N	Y	N	N	Y	N	Y
TERMINATOR	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
TESTER	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
THIMBLE	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
TIMEMARK	Y	N	N	Y	N	N	N	N	N	Y	N	N	N	N	N
TIMID	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
TIMOR	Y	N	Y	Y	N	N	N	N	N	Y	N	N	N	N	N
TINY	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
TINY DI	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
TINY FAMILY	Y	N	Y	N	N	N	N	N	N	Y	N	N	N	N	N
TOBACCO	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
TODOR	N	N	N	Y	N	N	N	Y	N	Y	N	N	N	N	N
TOKYO	N	N	N	Y	N	N	N	N	N	Y	N	N	N	N	N
TOLBUHIN	Y	N	Y	N	N	N	N	N	N	Y	N	N	N	N	N
TOMATO	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
TONY	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
TONY BOOT	Y	Y	N	N	N	Y	Y	N	N	N	N	N	Y	N	N
TOPO	Y	N	N	Y	N	N	N	N	N	Y	N	N	N	N	N
TORMENTOR	Y	N	N	Y	N	N	N	N	N	Y	N	N	N	N	N
TORMENTOR-205	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
TRACEBACK	Y	N	Y	Y	N	N	N	N	N	Y	N	N	N	N	N
TRACEBACK 3029	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
TRACEBACK II	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
TRAVELLER	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
TROI	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N

NAME	RES	MBR	COM	EXE	OVL	DOS BOOT	FD	CMD	O_W	PSITE	SPAWN	FAT	PART	STLTH	ENCRYPT
TULA	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
TUMEN	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
TURBO	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
TWIN PEAKS	N	N	Y	N	N	N	N	Y	Y	N	N	N	N	N	N
TWIN-351	Y	N	Y	Y	N	N	N	N	N	N	Y	N	N	N	N
TYPO BOOT	Y	Y	N	N	N	N	N	N	N	N	N	N	N	N	N
TYPO COM	Y	N	Y	N	N	N	N	N	N	Y	N	N	N	N	N
UNK	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
URFYDUS	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
USSR	N	N	N	Y	N	N	N	N	N	Y	N	N	N	N	N
USSR 1049	Y	N	Y	Y	N	N	N	N	N	Y	N	N	N	N	N
USSR 2144	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
USSR 311	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
USSR 492	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
USSR 516	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
USSR 600	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
USSR 707	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
USSR 711	Y	N	Y	N	N	N	N	N	N	Y	N	N	N	N	N
USSR 948	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
V-1N	N	N	Y	N	N	N	N	Y	Y	N	N	N	N	N	N
V-3N	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
V1024	Y	N	Y	Y	N	N	N	N	N	Y	N	N	N	N	N
V2000	Y	N	Y	Y	N	N	N	N	N	Y	N	N	N	N	Y
V2100	Y	N	Y	Y	Y	N	N	Y	N	Y	N	N	N	N	N
V270X	N	N	Y	N	N	N	N	N	N	Y	N	N	N	N	N
V2P2	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	Y
V2P6	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	Y
V483	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
V651	Y	N	Y	Y	N	N	N	N	N	Y	N	N	N	N	N
V800	Y	N	Y	N	N	N	N	N	N	Y	N	N	N	N	Y
V801	N	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
V82	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
VACSINA	Y	N	Y	Y	N	N	N	N	N	Y	N	N	N	N	N
VCL	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
VCOMM	Y	N	N	Y	N	N	N	N	N	Y	N	N	N	N	N
VCS	N	N	N	Y	N	N	N	N	N	Y	N	N	N	N	N
VFSI	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
VHP	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
VHP2	N	N	Y	N	N	N	N	N	N	Y	N	N	N	N	N
VICTOR	Y	N	Y	Y	Y	N	N	Y	N	Y	N	N	N	N	N
VIENNA	N	N	Y	N	N	N	N	N	N	Y	N	N	N	N	N
VINDICATOR	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
VIOLATOR	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
VIOLATOR B4	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
VIPER	N	N	Y	Y	N	N	N	Y	Y	N	N	N	N	N	N
VIPERIZE	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
VIRDEM	N	N	Y	N	N	N	N	N	N	Y	N	N	N	N	N
VIRDEM-1542	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
VIRDEM-792	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
VIRUS-101	Y	N	Y	Y	Y	Y	Y	Y	N	Y	N	N	N	N	Y

NAME	RES	MBR	COM	EXE	OVL	DOS BOOT	FD	CMD	O_W	PSITE	SPAWN	FAT	PART	STLTH	ENCR YPT
VIRUS-90	Y	N	Y	N	N	N	N	N	N	Y	N	N	N	N	N
VIVALDI	Y	N	N	Y	N	N	N	N	N	Y	N	N	N	N	N
VMEM	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	Y	N
VORONEZH	Y	N	Y	Y	N	N	N	N	N	Y	N	N	N	N	N
VORONEZH-370	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
VORONEZH-CHEMIST	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
VOTE	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
VP	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
VRIEST	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
VVF 3.4	Y	N	Y	Y	N	N	N	N	N	Y	N	N	N	N	N
W13	N	N	Y	N	N	N	N	N	N	N	N	N	N	N	N
WALKER	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
WARNING	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
WARRIOR	Y	N	N	Y	N	N	N	N	N	Y	N	N	N	N	N
WERE HERE	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
WESTWOOD	Y	N	Y	Y	Y	N	N	N	N	Y	N	N	N	N	N
WHALE	Y	N	Y	Y	N	N	N	N	N	Y	N	N	N	N	N
WINDMILL	Y	N	N	N	N	Y	Y	N	N	N	N	N	N	Y	N
WISCONSIN	N	N	Y	N	N	N	N	N	N	Y	N	N	N	N	N
WOLFMAN	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
WONDER	N	N	N	Y	N	N	N	N	Y	N	N	N	N	N	N
WONDERFUL	N	N	Y	N	N	N	N	N	N	Y	N	N	N	N	N
WORDSWAP	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
WORLD PEACE	Y	N	N	N	N	Y	Y	N	N	N	N	N	N	Y	N
WORM-16850	N	N	N	Y	N	N	N	N	N	N	Y	N	N	N	N
WORM-17690	N	N	N	Y	N	N	N	N	N	N	Y	N	N	N	N
WVIR	N	N	N	Y	N	N	N	N	N	Y	N	N	N	N	N
WWT	N	N	Y	N	N	N	N	Y	Y	N	N	N	N	N	N
XPEH	Y	N	Y	Y	N	N	N	N	N	Y	N	N	N	N	N
XUXA	Y	N	Y	N	N	N	N	N	N	Y	N	N	N	N	N
YAFO	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
YANKEE 2	N	N	N	Y	N	N	N	N	N	Y	N	N	N	N	N
YANKEE DOODLE	Y	N	Y	Y	N	N	N	N	N	Y	N	N	N	N	N
YAP	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	Y
YEAR 1992	Y	N	Y	Y	N	N	N	N	N	Y	N	N	N	N	N
YUKON OVERWRITING	N	N	Y	N	N	N	N	Y	Y	N	N	N	N	N	N
ZARAGOSA	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	Y	N
ZERO BUG	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
ZEROHUNT	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
ZHERKOV	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
ZK900	Y	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N
ZMT	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
ZUI	Y	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
ZY	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N
ZZ	N	N	Y	N	N	N	N	Y	N	Y	N	N	N	N	N

APPENDIX B - Selected fields showing classification results

VIRUS NAME	NODE NAME	SPLIT VARIABLES
405	1NNN	CMD. PSITE. RES
AIDS	1NNN	CMD. PSITE. RES
AIDS II	1NNN	CMD. PSITE. RES
CHRISTMAS TREE	1NNN	CMD. PSITE. RES
KAMIKAZI	1NNN	CMD. PSITE. RES
NUMBER ONE	1NNN	CMD. PSITE. RES
W13	1NNN	CMD. PSITE. RES
BOOT KILLER	1NNN	CMD. PSITE. RES
BUSTED	1NNN	CMD. PSITE. RES
CLONEWAR	1NNN	CMD. PSITE. RES
CRACKER JACK	1NNN	CMD. PSITE. RES
CRASH	1NNN	CMD. PSITE. RES
DEICIDE	1NNN	CMD. PSITE. RES
GLOBE	1NNN	CMD. PSITE. RES
GREEN PEACE	1NNN	CMD. PSITE. RES
HACKTIC	1NNN	CMD. PSITE. RES
HELLRAISER	1NNN	CMD. PSITE. RES
LANCS	1NNN	CMD. PSITE. RES
LZ	1NNN	CMD. PSITE. RES
MADISMO	1NNN	CMD. PSITE. RES
ONDRA	1NNN	CMD. PSITE. RES
PASCAL-4260	1NNN	CMD. PSITE. RES
QUIRK	1NNN	CMD. PSITE. RES
SKISM 1992	1NNN	CMD. PSITE. RES
WONDER	1NNN	CMD. PSITE. RES
WORM-16850	1NNN	CMD. PSITE. RES
WORM-17690	1NNN	CMD. PSITE. RES
AIRCOP	1NNY	CMD. PSITE. RES
ALAMEDA	1NNY	CMD. PSITE. RES
ASHAR	1NNY	CMD. PSITE. RES
BLOODY!	1NNY	CMD. PSITE. RES
BRAIN	1NNY	CMD. PSITE. RES
CHAOS	1NNY	CMD. PSITE. RES
DEN ZUK	1NNY	CMD. PSITE. RES
DISK KILLER	1NNY	CMD. PSITE. RES
EDV	1NNY	CMD. PSITE. RES
FORM	1NNY	CMD. PSITE. RES
JOSHI	1NNY	CMD. PSITE. RES
KOREA	1NNY	CMD. PSITE. RES
MARDI BROS	1NNY	CMD. PSITE. RES
MICROBES	1NNY	CMD. PSITE. RES
MUSICBUG	1NNY	CMD. PSITE. RES
OHIO	1NNY	CMD. PSITE. RES
PENTAGON	1NNY	CMD. PSITE. RES

VIRUS NAME	NODE NAME	SPLIT VARIABLES
PINGPONG	INNY	CMD, PSITE, RES
PRINT SCREEN	INNY	CMD, PSITE, RES
STONED	INNY	CMD, PSITE, RES
SUNDAY	INNY	CMD, PSITE, RES
SURIV 1.01	INNY	CMD, PSITE, RES
SWAP	INNY	CMD, PSITE, RES
TYPO BOOT	INNY	CMD, PSITE, RES
ANTI-TEL	INNY	CMD, PSITE, RES
ARAGON	INNY	CMD, PSITE, RES
AZUSA	INNY	CMD, PSITE, RES
BFD	INNY	CMD, PSITE, RES
CANNABIS	INNY	CMD, PSITE, RES
CANSU	INNY	CMD, PSITE, RES
CATMAN	INNY	CMD, PSITE, RES
CHANGU MANGU	INNY	CMD, PSITE, RES
CURSE BOOT	INNY	CMD, PSITE, RES
EVIL EMPIRE	INNY	CMD, PSITE, RES
EXEBUG	INNY	CMD, PSITE, RES
FILLER	INNY	CMD, PSITE, RES
FISH BOOT	INNY	CMD, PSITE, RES
GUILLON	INNY	CMD, PSITE, RES
HORSE BOOT	INNY	CMD, PSITE, RES
KEYDROP	INNY	CMD, PSITE, RES
LITTLE BROTHER	INNY	CMD, PSITE, RES
LOA DUONG	INNY	CMD, PSITE, RES
LOCKUP	INNY	CMD, PSITE, RES
MAX	INNY	CMD, PSITE, RES
MICHELANGELO	INNY	CMD, PSITE, RES
MUGSHOT	INNY	CMD, PSITE, RES
NOINT	INNY	CMD, PSITE, RES
QUEENS	INNY	CMD, PSITE, RES
SWEDISH DISASTER	INNY	CMD, PSITE, RES
TONY BOOT	INNY	CMD, PSITE, RES
TWIN-351	INNY	CMD, PSITE, RES
WINDMILL	INNY	CMD, PSITE, RES
WORLD PEACE	INNY	CMD, PSITE, RES
PLASTIQUE-B	INNY	CMD, PSITE, RES
1,226	INYN	CMD, PSITE, EXE
1,260	INYN	CMD, PSITE, EXE
AMBULANCE CAR	INYN	CMD, PSITE, EXE
AMSTRAD	INYN	CMD, PSITE, EXE
ARMAGEDDON	INYN	CMD, PSITE, EXE
CARIOCA	INYN	CMD, PSITE, EXE
CASCADE	INYN	CMD, PSITE, EXE
DATACRIME	INYN	CMD, PSITE, EXE
DBASE	INYN	CMD, PSITE, EXE
DEVIL'S DANCE	INYN	CMD, PSITE, EXE
DO-NOTHING	INYN	CMD, PSITE, EXE
FRIDAY 13TH COM	INYN	CMD, PSITE, EXE
GHOSTBALLS	INYN	CMD, PSITE, EXE

VIRUS NAME	NODE NAME	SPLIT VARIABLES
JOJO	1NYN	CMD, PSITE, EXE
JUNE 16TH	1NYN	CMD, PSITE, EXE
LISBON	1NYN	CMD, PSITE, EXE
OROPAX	1NYN	CMD, PSITE, EXE
RPVS	1NYN	CMD, PSITE, EXE
SOLANO 2000	1NYN	CMD, PSITE, EXE
TINY FAMILY	1NYN	CMD, PSITE, EXE
TYPO COM	1NYN	CMD, PSITE, EXE
USSR 711	1NYN	CMD, PSITE, EXE
V800	1NYN	CMD, PSITE, EXE
VHP2	1NYN	CMD, PSITE, EXE
VIENNA	1NYN	CMD, PSITE, EXE
VIRDEM	1NYN	CMD, PSITE, EXE
VIRUS-90	1NYN	CMD, PSITE, EXE
WISCONSIN	1NYN	CMD, PSITE, EXE
834	1NYN	CMD, PSITE, EXE
914	1NYN	CMD, PSITE, EXE
AH	1NYN	CMD, PSITE, EXE
ANT	1NYN	CMD, PSITE, EXE
ANTI-D	1NYN	CMD, PSITE, EXE
ARGENTINA	1NYN	CMD, PSITE, EXE
ATTACK	1NYN	CMD, PSITE, EXE
BARCELONA	1NYN	CMD, PSITE, EXE
BEWARE	1NYN	CMD, PSITE, EXE
BIG JOKE	1NYN	CMD, PSITE, EXE
BLIEC	1NYN	CMD, PSITE, EXE
CMDR BOMBER	1NYN	CMD, PSITE, EXE
DAD	1NYN	CMD, PSITE, EXE
EXUNT	1NYN	CMD, PSITE, EXE
FREEW-692	1NYN	CMD, PSITE, EXE
HIGHLANDER	1NYN	CMD, PSITE, EXE
I-B	1NYN	CMD, PSITE, EXE
ICE 9	1NYN	CMD, PSITE, EXE
INCOM	1NYN	CMD, PSITE, EXE
MACEDONIA	1NYN	CMD, PSITE, EXE
MANOLA	1NYN	CMD, PSITE, EXE
MINISTRY	1NYN	CMD, PSITE, EXE
NOBOCK	1NYN	CMD, PSITE, EXE
PHANTOM	1NYN	CMD, PSITE, EXE
PIAZOLLA	1NYN	CMD, PSITE, EXE
PIXEL	1NYN	CMD, PSITE, EXE
POGUE	1NYN	CMD, PSITE, EXE
QUIET	1NYN	CMD, PSITE, EXE
SIMULATI	1NYN	CMD, PSITE, EXE
STINKFOOT	1NYN	CMD, PSITE, EXE
STRIKER #1	1NYN	CMD, PSITE, EXE
TELECOM	1NYN	CMD, PSITE, EXE
TOLBUHIN	1NYN	CMD, PSITE, EXE
V270X	1NYN	CMD, PSITE, EXE
WONDERFUL	1NYN	CMD, PSITE, EXE

VIRUS NAME	NODE NAME	SPLIT VARIABLES
XUXA	1NYN	CMD, PSITE, EXE
SYLVIA	1NYN	CMD, PSITE, EXE
337	1NYN	CMD, PSITE, EXE
BETA	1NYN	CMD, PSITE, EXE
1,210	1NYY	CMD, PSITE, EXE
1,381	1NYY	CMD, PSITE, EXE
1,605	1NYY	CMD, PSITE, EXE
1,720	1NYY	CMD, PSITE, EXE
4,096	1NYY	CMD, PSITE, EXE
ALABAMA	1NYY	CMD, PSITE, EXE
EIGHT TUNES	1NYY	CMD, PSITE, EXE
FELLOWSHIP	1NYY	CMD, PSITE, EXE
FLASH	1NYY	CMD, PSITE, EXE
FRERE JACQUES	1NYY	CMD, PSITE, EXE
FU MANCHU	1NYY	CMD, PSITE, EXE
GROEN LINKS	1NYY	CMD, PSITE, EXE
HALLOECHEN	1NYY	CMD, PSITE, EXE
ICELANDIC	1NYY	CMD, PSITE, EXE
INVADER	1NYY	CMD, PSITE, EXE
ITAVIR	1NYY	CMD, PSITE, EXE
JERUSALEM	1NYY	CMD, PSITE, EXE
JOKER	1NYY	CMD, PSITE, EXE
JULY 13TH	1NYY	CMD, PSITE, EXE
MIRROR	1NYY	CMD, PSITE, EXE
MIX1	1NYY	CMD, PSITE, EXE
PLASTIQUE	1NYY	CMD, PSITE, EXE
SATURDAY THE 14TH	1NYY	CMD, PSITE, EXE
SCOTTS VALLEY	1NYY	CMD, PSITE, EXE
SLOW	1NYY	CMD, PSITE, EXE
SPYER	1NYY	CMD, PSITE, EXE
SURIV 2.01	1NYY	CMD, PSITE, EXE
SURIV 3.00	1NYY	CMD, PSITE, EXE
SVIR	1NYY	CMD, PSITE, EXE
SYSLOCK	1NYY	CMD, PSITE, EXE
TAIWAN 3	1NYY	CMD, PSITE, EXE
TAIWAN 4	1NYY	CMD, PSITE, EXE
TRACEBACK	1NYY	CMD, PSITE, EXE
USSR	1NYY	CMD, PSITE, EXE
USSR 1049	1NYY	CMD, PSITE, EXE
V651	1NYY	CMD, PSITE, EXE
V1024	1NYY	CMD, PSITE, EXE
V2000	1NYY	CMD, PSITE, EXE
VACSINA	1NYY	CMD, PSITE, EXE
VCOMM	1NYY	CMD, PSITE, EXE
VORONEZH	1NYY	CMD, PSITE, EXE
WESTWOOD	1NYY	CMD, PSITE, EXE
WHALE	1NYY	CMD, PSITE, EXE
YANKEE DOODLE	1NYY	CMD, PSITE, EXE
YANKEE 2	1NYY	CMD, PSITE, EXE
1557	1NYY	CMD, PSITE, EXE

VIRUS NAME	NODE NAME	SPLIT VARIABLES
572	INYY	CMD, PSITE, EXE
981	INYY	CMD, PSITE, EXE
1,244	INYY	CMD, PSITE, EXE
1,835	INYY	CMD, PSITE, EXE
2,153	INYY	CMD, PSITE, EXE
2,559	INYY	CMD, PSITE, EXE
2,560	INYY	CMD, PSITE, EXE
2,623	INYY	CMD, PSITE, EXE
3,445	INYY	CMD, PSITE, EXE
7,808	INYY	CMD, PSITE, EXE
ANDRE	INYY	CMD, PSITE, EXE
AUSTRALIAN	INYY	CMD, PSITE, EXE
BADSEC	INYY	CMD, PSITE, EXE
BANDIT	INYY	CMD, PSITE, EXE
BAOBAB	INYY	CMD, PSITE, EXE
BLACK WIZARD	INYY	CMD, PSITE, EXE
BOOJUM	INYY	CMD, PSITE, EXE
CARFIELD	INYY	CMD, PSITE, EXE
CD	INYY	CMD, PSITE, EXE
CHASER	INYY	CMD, PSITE, EXE
CLOSE	INYY	CMD, PSITE, EXE
COFFEESHOP-1568	INYY	CMD, PSITE, EXE
COSSIGA	INYY	CMD, PSITE, EXE
DADA	INYY	CMD, PSITE, EXE
DAVIS	INYY	CMD, PSITE, EXE
DISCOM	INYY	CMD, PSITE, EXE
EINSTEIN	INYY	CMD, PSITE, EXE
ENIGMA	INYY	CMD, PSITE, EXE
ENOLA	INYY	CMD, PSITE, EXE
ERROR	INYY	CMD, PSITE, EXE
FLOWER	INYY	CMD, PSITE, EXE
FORGER	INYY	CMD, PSITE, EXE
FRIENDS	INYY	CMD, PSITE, EXE
GOT-YOU	INYY	CMD, PSITE, EXE
HAFENSTRASS	INYY	CMD, PSITE, EXE
HELLWEEN	INYY	CMD, PSITE, EXE
HERO	INYY	CMD, PSITE, EXE
HERO-394	INYY	CMD, PSITE, EXE
HI	INYY	CMD, PSITE, EXE
IDLE	INYY	CMD, PSITE, EXE
INTRUDER	INYY	CMD, PSITE, EXE
INVOL	INYY	CMD, PSITE, EXE
JERUSALEM 11-30	INYY	CMD, PSITE, EXE
JOKER 2	INYY	CMD, PSITE, EXE
KEYBOARD BUG	INYY	CMD, PSITE, EXE
KLAEREN	INYY	CMD, PSITE, EXE
KRIVMOUS	INYY	CMD, PSITE, EXE
LEGALIZE	INYY	CMD, PSITE, EXE
LITTLE PIECES	INYY	CMD, PSITE, EXE
MALAGA	INYY	CMD, PSITE, EXE

VIRUS NAME	NODE NAME	SPLIT VARIABLES
MICROPOX	1NYY	CMD. PSITE. EXE
MIKY	1NYY	CMD. PSITE. EXE
MIX2	1NYY	CMD. PSITE. EXE
MOSQUITO	1NYY	CMD. PSITE. EXE
MPS 4.01	1NYY	CMD. PSITE. EXE
MUMMY	1NYY	CMD. PSITE. EXE
NYGUS	1NYY	CMD. PSITE. EXE
ONTARIO-730	1NYY	CMD. PSITE. EXE
PA	1NYY	CMD. PSITE. EXE
PATHHUNT	1NYY	CMD. PSITE. EXE
PATIENT	1NYY	CMD. PSITE. EXE
PCV	1NYY	CMD. PSITE. EXE
PI	1NYY	CMD. PSITE. EXE
PILA	1NYY	CMD. PSITE. EXE
PISELLO	1NYY	CMD. PSITE. EXE
QUAKE	1NYY	CMD. PSITE. EXE
RETURNS	1NYY	CMD. PSITE. EXE
RNA	1NYY	CMD. PSITE. EXE
SADIST	1NYY	CMD. PSITE. EXE
SHIELD	1NYY	CMD. PSITE. EXE
SLAYER FAMILY	1NYY	CMD. PSITE. EXE
SLOVAK	1NYY	CMD. PSITE. EXE
SPANISH APRIL FOOLS	1NYY	CMD. PSITE. EXE
STARDOT 600	1NYY	CMD. PSITE. EXE
SVC 6.0	1NYY	CMD. PSITE. EXE
TABULERO	1NYY	CMD. PSITE. EXE
TEQUILA	1NYY	CMD. PSITE. EXE
TIMEMARK	1NYY	CMD. PSITE. EXE
TIMOR	1NYY	CMD. PSITE. EXE
TOKYO	1NYY	CMD. PSITE. EXE
TOPO	1NYY	CMD. PSITE. EXE
TORMENTOR	1NYY	CMD. PSITE. EXE
VCS	1NYY	CMD. PSITE. EXE
VIVALDI	1NYY	CMD. PSITE. EXE
VVF 3.4	1NYY	CMD. PSITE. EXE
WARRIOR	1NYY	CMD. PSITE. EXE
WVIR	1NYY	CMD. PSITE. EXE
XPEH	1NYY	CMD. PSITE. EXE
YEAR 1992	1NYY	CMD. PSITE. EXE
MALTESE AMOEBA	1NYY	CMD. PSITE. EXE
646	1YNN	CMD. RES. O_W
5.120	1YNN	CMD. RES. O_W
ANTI-PASCAL	1YNN	CMD. RES. O_W
ANTI-PASCAL II	1YNN	CMD. RES. O_W
BLOOD	1YNN	CMD. RES. O_W
CASPER	1YNN	CMD. RES. O_W
CHRISTMAS IN JAPAN	1YNN	CMD. RES. O_W
DOT KILLER	1YNN	CMD. RES. O_W
FATHER XMAS	1YNN	CMD. RES. O_W
JEFF	1YNN	CMD. RES. O_W

VIRUS NAME	NODE NAME	SPLIT VARIABLES
KEMEROVO	1YNN	CMD, RES, O_W
MGTU	1YNN	CMD, RES, O_W
PARIS	1YNN	CMD, RES, O_W
PERFUME	1YNN	CMD, RES, O_W
POLIMER	1YNN	CMD, RES, O_W
POLISH 217	1YNN	CMD, RES, O_W
POLISH 583	1YNN	CMD, RES, O_W
STONE '90	1YNN	CMD, RES, O_W
TAIWAN	1YNN	CMD, RES, O_W
TINY	1YNN	CMD, RES, O_W
V2P2	1YNN	CMD, RES, O_W
V2P6	1YNN	CMD, RES, O_W
VFSI	1YNN	CMD, RES, O_W
VHP	1YNN	CMD, RES, O_W
VIOLATOR	1YNN	CMD, RES, O_W
VP	1YNN	CMD, RES, O_W
595	1YNN	CMD, RES, O_W
621	1YNN	CMD, RES, O_W
1,308	1YNN	CMD, RES, O_W
ADOLPH	1YNN	CMD, RES, O_W
AFRICAN 109	1YNN	CMD, RES, O_W
AKUKU	1YNN	CMD, RES, O_W
ALBANIA	1YNN	CMD, RES, O_W
ANTIMON	1YNN	CMD, RES, O_W
ANTO	1YNN	CMD, RES, O_W
ARF	1YNN	CMD, RES, O_W
ASII	1YNN	CMD, RES, O_W
ATAS	1YNN	CMD, RES, O_W
AUGUST 16TH	1YNN	CMD, RES, O_W
BEAST-N-BLACK	1YNN	CMD, RES, O_W
BOB	1YNN	CMD, RES, O_W
BRAZILIAN BUG	1YNN	CMD, RES, O_W
CADKILL	1YNN	CMD, RES, O_W
CHAD	1YNN	CMD, RES, O_W
CREW-2480	1YNN	CMD, RES, O_W
CRF	1YNN	CMD, RES, O_W
CV4	1YNN	CMD, RES, O_W
CYBER	1YNN	CMD, RES, O_W
DAME (DARK AVENGER MUT MACH)	1YNN	CMD, RES, O_W
DAY10	1YNN	CMD, RES, O_W
DEST	1YNN	CMD, RES, O_W
DEWDZ	1YNN	CMD, RES, O_W
DIMA	1YNN	CMD, RES, O_W
EAR	1YNN	CMD, RES, O_W
ELIZA	1YNN	CMD, RES, O_W
EMF	1YNN	CMD, RES, O_W
FATHER CHRISTMAS	1YNN	CMD, RES, O_W
FGT	1YNN	CMD, RES, O_W
FRODO SOFT	1YNN	CMD, RES, O_W

VIRUS NAME	NODE NAME	SPLIT VARIABLES
GERGANA	1YNN	CMD, RES, O_W
GLISS	1YNN	CMD, RES, O_W
GRAPJE	1YNN	CMD, RES, O_W
GREEN JOKER	1YNN	CMD, RES, O_W
GRITHER	1YNN	CMD, RES, O_W
GRUNT-1	1YNN	CMD, RES, O_W
HALLOWEEN	1YNN	CMD, RES, O_W
HAPPY	1YNN	CMD, RES, O_W
HELL	1YNN	CMD, RES, O_W
HOMINY	1YNN	CMD, RES, O_W
HYBRYD	1YNN	CMD, RES, O_W
HYDRA FAMILY	1YNN	CMD, RES, O_W
IKV 528	1YNN	CMD, RES, O_W
ILL	1YNN	CMD, RES, O_W
INFINITY	1YNN	CMD, RES, O_W
INTERCEPTOR	1YNN	CMD, RES, O_W
IRAQUI WARRIOR	1YNN	CMD, RES, O_W
IT	1YNN	CMD, RES, O_W
ITALIAN 803	1YNN	CMD, RES, O_W
JERK	1YNN	CMD, RES, O_W
JULY 26TH	1YNN	CMD, RES, O_W
KARIN	1YNN	CMD, RES, O_W
KIEV 483	1YNN	CMD, RES, O_W
KODE4	1YNN	CMD, RES, O_W
KUKU-448	1YNN	CMD, RES, O_W
LOWERCASE	1YNN	CMD, RES, O_W
MANTA	1YNN	CMD, RES, O_W
MARAUDER	1YNN	CMD, RES, O_W
MARL	1YNN	CMD, RES, O_W
MEDICAL	1YNN	CMD, RES, O_W
MONXLA B	1YNN	CMD, RES, O_W
MPS 3.2	1YNN	CMD, RES, O_W
MPS 1.1	1YNN	CMD, RES, O_W
MPS 3.1	1YNN	CMD, RES, O_W
MSHARK	1YNN	CMD, RES, O_W
MSTU	1YNN	CMD, RES, O_W
MULTI-123	1YNN	CMD, RES, O_W
MUNICH	1YNN	CMD, RES, O_W
NTKC	1YNN	CMD, RES, O_W
NULL SET	1YNN	CMD, RES, O_W
NULL-178	1YNN	CMD, RES, O_W
OMT	1YNN	CMD, RES, O_W
OTTO6	1YNN	CMD, RES, O_W
PADDED	1YNN	CMD, RES, O_W
PARASITE	1YNN	CMD, RES, O_W
PARITY	1YNN	CMD, RES, O_W
PARTICLE MAN	1YNN	CMD, RES, O_W
PATH	1YNN	CMD, RES, O_W
PIXIE	1YNN	CMD, RES, O_W
PLUTTO	1YNN	CMD, RES, O_W

VIRUS NAME	NODE NAME	SPLIT VARIABLES
POLISH-376	1YNN	CMD, RES, O_W
PRIME	1YNN	CMD, RES, O_W
RAGE	1YNN	CMD, RES, O_W
RAUBKOPIE	1YNN	CMD, RES, O_W
REBOOT	1YNN	CMD, RES, O_W
RELZFU	1YNN	CMD, RES, O_W
RESET	1YNN	CMD, RES, O_W
ROSEN	1YNN	CMD, RES, O_W
SAD	1YNN	CMD, RES, O_W
SELF	1YNN	CMD, RES, O_W
SEVENTH SON	1YNN	CMD, RES, O_W
SHADOW	1YNN	CMD, RES, O_W
SICILIAN MOB	1YNN	CMD, RES, O_W
SILLY WILLY	1YNN	CMD, RES, O_W
SILLY	1YNN	CMD, RES, O_W
SILLY-365	1YNN	CMD, RES, O_W
SOV	1YNN	CMD, RES, O_W
SPANZ	1YNN	CMD, RES, O_W
STAF	1YNN	CMD, RES, O_W
STAHL	1YNN	CMD, RES, O_W
STANCO	1YNN	CMD, RES, O_W
STARDOT 801	1YNN	CMD, RES, O_W
STARDOT 789	1YNN	CMD, RES, O_W
STUPID-1355	1YNN	CMD, RES, O_W
SWEDISH BOYS	1YNN	CMD, RES, O_W
SWISS 143	1YNN	CMD, RES, O_W
TACK	1YNN	CMD, RES, O_W
TALENTLESS	1YNN	CMD, RES, O_W
TESTER	1YNN	CMD, RES, O_W
TIMID	1YNN	CMD, RES, O_W
TINY DI	1YNN	CMD, RES, O_W
TODOR	1YNN	CMD, RES, O_W
TONY	1YNN	CMD, RES, O_W
TORMENTOR-205	1YNN	CMD, RES, O_W
USSR 311	1YNN	CMD, RES, O_W
V-3N	1YNN	CMD, RES, O_W
V801	1YNN	CMD, RES, O_W
VCL	1YNN	CMD, RES, O_W
VIOLATOR B4	1YNN	CMD, RES, O_W
VIPERIZE	1YNN	CMD, RES, O_W
VIRDEM-1542	1YNN	CMD, RES, O_W
VIRDEM-792	1YNN	CMD, RES, O_W
VOTE	1YNN	CMD, RES, O_W
WARNING	1YNN	CMD, RES, O_W
WERE HERE	1YNN	CMD, RES, O_W
YAFO	1YNN	CMD, RES, O_W
ZY	1YNN	CMD, RES, O_W
ZZ	1YNN	CMD, RES, O_W
66A	1YNN	CMD, RES, O_W
382	1YNY	CMD, RES, O_W

VIRUS NAME	NODE NAME	SPLIT VARIABLES
BURGER	1YNY	CMD, RES, O_W
LEPROSY	1YNY	CMD, RES, O_W
4,870	1YNY	CMD, RES, O_W
ACID	1YNY	CMD, RES, O_W
BAD BRAIN	1YNY	CMD, RES, O_W
BANANA	1YNY	CMD, RES, O_W
BLOOD LUST	1YNY	CMD, RES, O_W
DEFINE	1YNY	CMD, RES, O_W
EXPLODE	1YNY	CMD, RES, O_W
FCB	1YNY	CMD, RES, O_W
HARAKIRI	1YNY	CMD, RES, O_W
HASTINGS	1YNY	CMD, RES, O_W
ITTI	1YNY	CMD, RES, O_W
MALMSEY	1YNY	CMD, RES, O_W
MINI-45	1YNY	CMD, RES, O_W
MUTANT FAMILY	1YNY	CMD, RES, O_W
NOWHERE MAN	1YNY	CMD, RES, O_W
PASCAL-5220	1YNY	CMD, RES, O_W
PIRATE	1YNY	CMD, RES, O_W
POLISH-45	1YNY	CMD, RES, O_W
POSSUM	1YNY	CMD, RES, O_W
PS-MPC	1YNY	CMD, RES, O_W
PSYCHOGENIUS	1YNY	CMD, RES, O_W
SHHS	1YNY	CMD, RES, O_W
SILVER DOLLAR	1YNY	CMD, RES, O_W
SMALL-38	1YNY	CMD, RES, O_W
TWIN PEAKS	1YNY	CMD, RES, O_W
V-1N	1YNY	CMD, RES, O_W
VIPER	1YNY	CMD, RES, O_W
WWT	1YNY	CMD, RES, O_W
YUKON OVERWRITING	1YNY	CMD, RES, O_W
ANTHRAX	1YYN	CMD, RES, PSITE
LEHIGH	1YYN	CMD, RES, PSITE
NOMENKLATURA	1YYN	CMD, RES, PSITE
SVERDLOV	1YYN	CMD, RES, PSITE
BLAZE	1YYN	CMD, RES, PSITE
CRAZY EDDIE	1YYN	CMD, RES, PSITE
DARTH VADER	1YYN	CMD, RES, PSITE
DIR-2	1YYN	CMD, RES, PSITE
LABEL	1YYN	CMD, RES, PSITE
QMU	1YYN	CMD, RES, PSITE
SQUISHER	1YYN	CMD, RES, PSITE
512	1YYY	CMD, RES, PSITE
1,008	1YYY	CMD, RES, PSITE
1,253	1YYY	CMD, RES, PSITE
1,392	1YYY	CMD, RES, PSITE
ATTENTION!	1YYY	CMD, RES, PSITE
BEST WISHES	1YYY	CMD, RES, PSITE
BLACK MONDAY	1YYY	CMD, RES, PSITE
DARK AVENGER	1YYY	CMD, RES, PSITE

VIRUS NAME	NODE NAME	SPLIT VARIABLES
DATALOCK	1YYY	CMD, RES, PSITE
EVIL	1YYY	CMD, RES, PSITE
FISH	1YYY	CMD, RES, PSITE
FLIP	1YYY	CMD, RES, PSITE
GUPPY	1YYY	CMD, RES, PSITE
HOLOCAUST	1YYY	CMD, RES, PSITE
HYMN	1YYY	CMD, RES, PSITE
KEYPRESS	1YYY	CMD, RES, PSITE
LIBERTY	1YYY	CMD, RES, PSITE
LOZINSKY	1YYY	CMD, RES, PSITE
MONXLA	1YYY	CMD, RES, PSITE
MURPHY	1YYY	CMD, RES, PSITE
ONTARIO	1YYY	CMD, RES, PSITE
PHOENIX	1YYY	CMD, RES, PSITE
PHOENIXD	1YYY	CMD, RES, PSITE
POLISH 529	1YYY	CMD, RES, PSITE
PROUD	1YYY	CMD, RES, PSITE
RED DIAVOLYATA	1YYY	CMD, RES, PSITE
SHAKE	1YYY	CMD, RES, PSITE
SOURY	1YYY	CMD, RES, PSITE
TRACEBACK II	1YYY	CMD, RES, PSITE
USSR 516	1YYY	CMD, RES, PSITE
USSR 600	1YYY	CMD, RES, PSITE
USSR 948	1YYY	CMD, RES, PSITE
USSR 2144	1YYY	CMD, RES, PSITE
V2100	1YYY	CMD, RES, PSITE
VICTOR	1YYY	CMD, RES, PSITE
WOLFMAN	1YYY	CMD, RES, PSITE
ZERO BUG	1YYY	CMD, RES, PSITE
ZEROHUNT	1YYY	CMD, RES, PSITE
408	1YYY	CMD, RES, PSITE
439	1YYY	CMD, RES, PSITE
500	1YYY	CMD, RES, PSITE
923	1YYY	CMD, RES, PSITE
1024 PRINT SCREEN	1YYY	CMD, RES, PSITE
1024 SBC	1YYY	CMD, RES, PSITE
1,067	1YYY	CMD, RES, PSITE
1,241	1YYY	CMD, RES, PSITE
1,385	1YYY	CMD, RES, PSITE
1,452	1YYY	CMD, RES, PSITE
1,575	1YYY	CMD, RES, PSITE
1,661	1YYY	CMD, RES, PSITE
1,840	1YYY	CMD, RES, PSITE
1,963	1YYY	CMD, RES, PSITE
ADA	1YYY	CMD, RES, PSITE
AGENA	1YYY	CMD, RES, PSITE
ALEXANDER	1YYY	CMD, RES, PSITE
ALFA	1YYY	CMD, RES, PSITE
ALL SYS 9	1YYY	CMD, RES, PSITE
ANIMUS	1YYY	CMD, RES, PSITE

VIRUS NAME	NODE NAME	SPLIT VARIABLES
ARKANOID	1YYY	CMD, RES, PSITE
ASP-472	1YYY	CMD, RES, PSITE
ASTRA	1YYY	CMD, RES, PSITE
AT144	1YYY	CMD, RES, PSITE
ATHENS	1YYY	CMD, RES, PSITE
AUSTRALIAN 403	1YYY	CMD, RES, PSITE
BACKTIME	1YYY	CMD, RES, PSITE
BAD BOY	1YYY	CMD, RES, PSITE
BEBE	1YYY	CMD, RES, PSITE
BLINKER	1YYY	CMD, RES, PSITE
BOMBER	1YYY	CMD, RES, PSITE
BOW	1YYY	CMD, RES, PSITE
BOYS	1YYY	CMD, RES, PSITE
BRAINY	1YYY	CMD, RES, PSITE
BURGHOFER	1YYY	CMD, RES, PSITE
CAPITALL	1YYY	CMD, RES, PSITE
CARA	1YYY	CMD, RES, PSITE
CASINO	1YYY	CMD, RES, PSITE
CAZ	1YYY	CMD, RES, PSITE
CB-1530	1YYY	CMD, RES, PSITE
CERBURUS	1YYY	CMD, RES, PSITE
CHANG	1YYY	CMD, RES, PSITE
CHECKSUM	1YYY	CMD, RES, PSITE
CHEEBA	1YYY	CMD, RES, PSITE
CHEMMY	1YYY	CMD, RES, PSITE
CINDERELLA	1YYY	CMD, RES, PSITE
COPYRIGHT	1YYY	CMD, RES, PSITE
CRAZY IMP	1YYY	CMD, RES, PSITE
CREEPER	1YYY	CMD, RES, PSITE
CRIMINAL	1YYY	CMD, RES, PSITE
CSL	1YYY	CMD, RES, PSITE
DAMAGE	1YYY	CMD, RES, PSITE
DARK LORD	1YYY	CMD, RES, PSITE
DEMOLITION	1YYY	CMD, RES, PSITE
DESTRUCTOR V4.0	1YYY	CMD, RES, PSITE
DIR VIRUS	1YYY	CMD, RES, PSITE
DM	1YYY	CMD, RES, PSITE
DODO	1YYY	CMD, RES, PSITE
DOOM II	1YYY	CMD, RES, PSITE
DUTCH 555	1YYY	CMD, RES, PSITE
DUTCH TINY	1YYY	CMD, RES, PSITE
EDEL	1YYY	CMD, RES, PSITE
EMMIE	1YYY	CMD, RES, PSITE
END OF	1YYY	CMD, RES, PSITE
ENEMY	1YYY	CMD, RES, PSITE
ETC	1YYY	CMD, RES, PSITE
EUROPE-92	1YYY	CMD, RES, PSITE
FATHER	1YYY	CMD, RES, PSITE
FEIST	1YYY	CMD, RES, PSITE
FICH	1YYY	CMD, RES, PSITE

VIRUS NAME	NODE NAME	SPLIT VARIABLES
FICHV-896	1YYY	CMD, RES, PSITE
FIL	1YYY	CMD, RES, PSITE
FINGERS	1YYY	CMD, RES, PSITE
FINNISH-709	1YYY	CMD, RES, PSITE
FROGS	1YYY	CMD, RES, PSITE
FUNERAL	1YYY	CMD, RES, PSITE
FUNGUS	1YYY	CMD, RES, PSITE
GEEK	1YYY	CMD, RES, PSITE
GNOSE	1YYY	CMD, RES, PSITE
GOSIA	1YYY	CMD, RES, PSITE
GOTCHA	1YYY	CMD, RES, PSITE
GREMLIN	1YYY	CMD, RES, PSITE
GROOVE	1YYY	CMD, RES, PSITE
GROWING BLOCK	1YYY	CMD, RES, PSITE
HA	1YYY	CMD, RES, PSITE
HAIFA	1YYY	CMD, RES, PSITE
HAPPY NEW YEAR	1YYY	CMD, RES, PSITE
HARY ANTO	1YYY	CMD, RES, PSITE
HH&H	1YYY	CMD, RES, PSITE
HITCHCOCK	1YYY	CMD, RES, PSITE
HORROR	1YYY	CMD, RES, PSITE
HUNGARIAN	1YYY	CMD, RES, PSITE
HUNGARIAN 482	1YYY	CMD, RES, PSITE
JD	1YYY	CMD, RES, PSITE
JERUSALEM 1767	1YYY	CMD, RES, PSITE
JOANNA	1YYY	CMD, RES, PSITE
JOJO 2	1YYY	CMD, RES, PSITE
JW2	1YYY	CMD, RES, PSITE
KALAH	1YYY	CMD, RES, PSITE
KIT	1YYY	CMD, RES, PSITE
LAZY	1YYY	CMD, RES, PSITE
LEECH	1YYY	CMD, RES, PSITE
LIBERTY-1172	1YYY	CMD, RES, PSITE
LIBERTY-2	1YYY	CMD, RES, PSITE
LITTLE GIRL	1YYY	CMD, RES, PSITE
LUCIFER	1YYY	CMD, RES, PSITE
LYCEE	1YYY	CMD, RES, PSITE
M.I.R.	1YYY	CMD, RES, PSITE
MAGNITOGORSK 2048	1YYY	CMD, RES, PSITE
MALAISE	1YYY	CMD, RES, PSITE
MANNEQUIN	1YYY	CMD, RES, PSITE
MAYAK	1YYY	CMD, RES, PSITE
MEXICAN MUD	1YYY	CMD, RES, PSITE
MG	1YYY	CMD, RES, PSITE
MICRO 128	1YYY	CMD, RES, PSITE
MILENA	1YYY	CMD, RES, PSITE
MINSK GHOST	1YYY	CMD, RES, PSITE
MOCTEZUMA'S REVENGE	1YYY	CMD, RES, PSITE
MONO	1YYY	CMD, RES, PSITE
MONTH 4-6	1YYY	CMD, RES, PSITE

VIRUS NAME	NODE NAME	SPLIT VARIABLES
MULE	1YYY	CMD, RES, PSITE
MULTI-FACE	1YYY	CMD, RES, PSITE
NAUGHTY HACKER	1YYY	CMD, RES, PSITE
NEWCOM	1YYY	CMD, RES, PSITE
NINA	1YYY	CMD, RES, PSITE
NINES	1YYY	CMD, RES, PSITE
NO FRILLS	1YYY	CMD, RES, PSITE
NOVEMBER 17TH	1YYY	CMD, RES, PSITE
NPOX	1YYY	CMD, RES, PSITE
ONTARIO III	1YYY	CMD, RES, PSITE
PC FLU	1YYY	CMD, RES, PSITE
PC FLU-2	1YYY	CMD, RES, PSITE
PCBB	1YYY	CMD, RES, PSITE
PENZA	1YYY	CMD, RES, PSITE
PHOENIX 2000	1YYY	CMD, RES, PSITE
PIF	1YYY	CMD, RES, PSITE
PITCH	1YYY	CMD, RES, PSITE
PLOVDIV 1.1	1YYY	CMD, RES, PSITE
PLOVDIV 1.3	1YYY	CMD, RES, PSITE
PROBLEM	1YYY	CMD, RES, PSITE
POEM	1YYY	CMD, RES, PSITE
POJER	1YYY	CMD, RES, PSITE
POSSESSED	1YYY	CMD, RES, PSITE
PREGNANT	1YYY	CMD, RES, PSITE
PROTECTO	1YYY	CMD, RES, PSITE
QP3	1YYY	CMD, RES, PSITE
R-10	1YYY	CMD, RES, PSITE
R-11	1YYY	CMD, RES, PSITE
RAM VIRUS	1YYY	CMD, RES, PSITE
RATTLE	1YYY	CMD, RES, PSITE
REKLAMA	1YYY	CMD, RES, PSITE
REVENGE ATTACKER	1YYY	CMD, RES, PSITE
ROCKO	1YYY	CMD, RES, PSITE
RSP-1876	1YYY	CMD, RES, PSITE
RYBKA	1YYY	CMD, RES, PSITE
SADDAM	1YYY	CMD, RES, PSITE
SCREAM	1YYY	CMD, RES, PSITE
SEMTEX	1YYY	CMD, RES, PSITE
SENTINEL	1YYY	CMD, RES, PSITE
SHAKER	1YYY	CMD, RES, PSITE
SILENCE	1YYY	CMD, RES, PSITE
SISKIN	1YYY	CMD, RES, PSITE
SISTOR	1YYY	CMD, RES, PSITE
SMILEY	1YYY	CMD, RES, PSITE
SOMETHING	1YYY	CMD, RES, PSITE
SPANISH	1YYY	CMD, RES, PSITE
SPARSE	1YYY	CMD, RES, PSITE
SQUAWK	1YYY	CMD, RES, PSITE
SQUEAKER	1YYY	CMD, RES, PSITE
STICKY	1YYY	CMD, RES, PSITE

VIRUS NAME	NODE NAME	SPLIT VARIABLES
SUNDAY-2	1YYY	CMD, RES, PSITE
SURRENDER	1YYY	CMD, RES, PSITE
SVC 3.1	1YYY	CMD, RES, PSITE
SVC 4.0	1YYY	CMD, RES, PSITE
SVC 5.0	1YYY	CMD, RES, PSITE
SWISS PHOENIX	1YYY	CMD, RES, PSITE
TENBYTES	1YYY	CMD, RES, PSITE
TERMINATOR	1YYY	CMD, RES, PSITE
THIMBLE	1YYY	CMD, RES, PSITE
TOBACCO	1YYY	CMD, RES, PSITE
TOMATO	1YYY	CMD, RES, PSITE
TRACEBACK 3029	1YYY	CMD, RES, PSITE
TRAVELLER	1YYY	CMD, RES, PSITE
TROI	1YYY	CMD, RES, PSITE
TUMEN	1YYY	CMD, RES, PSITE
TURBO	1YYY	CMD, RES, PSITE
UNK	1YYY	CMD, RES, PSITE
URFYDUS	1YYY	CMD, RES, PSITE
USSR 707	1YYY	CMD, RES, PSITE
USSR 492	1YYY	CMD, RES, PSITE
V483	1YYY	CMD, RES, PSITE
V82	1YYY	CMD, RES, PSITE
VIRUS-101	1YYY	CMD, RES, PSITE
VMEM	1YYY	CMD, RES, PSITE
VORONEZH-370	1YYY	CMD, RES, PSITE
VORONEZH-CHEMIST	1YYY	CMD, RES, PSITE
VRIEST	1YYY	CMD, RES, PSITE
WALKER	1YYY	CMD, RES, PSITE
WORDSWAP	1YYY	CMD, RES, PSITE
YAP	1YYY	CMD, RES, PSITE
ZARAGOSA	1YYY	CMD, RES, PSITE
ZHERKOV	1YYY	CMD, RES, PSITE
ZK900	1YYY	CMD, RES, PSITE
ZMT	1YYY	CMD, RES, PSITE
ZU1	1YYY	CMD, RES, PSITE
TULA	1YYY	CMD, RES, PSITE
VINDICATOR	1YYY	CMD, RES, PSITE
ZARAGOSA	1YYY	CMD, RES, PSITE
ZHERKOV	1YYY	CMD, RES, PSITE
ZK900	1YYY	CMD, RES, PSITE
ZMT	1YYY	CMD, RES, PSITE
ZU1	1YYY	CMD, RES, PSITE

APPENDIX C - MONOFLDS database contents (temporary processing information)

FIELDNAME	CURRENT	USED	COMP_SCORE	ORDERED
EXE	N	N	0	N
RES	N	N	0	N
COM	N	N	0	N
MBR	N	N	0	N
PSITE	N	N	0	N
O_W	N	N	0	N
CMD	N	N	0	N

APPENDIX D - NODEVARS database contents (processing progress record & depth control)

NODENAME	EXE	COM	RES	MBR	PSITE	O_W	CMD	NODE PASSED	NODE LEVEL	FILTER
1	N	N	N	N	N	N	Y	Y	1	CMD
1Y	N	N	Y	N	N	N	Y	Y	2	CMD, RES
1N	N	N	N	N	Y	N	Y	Y	2	CMD. PSITE
1YY	N	N	Y	N	Y	N	Y	Y	3	CMD. RES. PSITE
1YN	N	N	Y	N	N	Y	Y	Y	3	CMD, RES. O_W
1NY	Y	N	N	N	Y	N	Y	Y	3	CMD. PSITE. EXE
1NN	N	N	Y	N	Y	N	Y	Y	3	CMD, PSITE, RES

APPENDIX E - Monothetic analysis program

```
;;  This program is to group data referring to computer virus characteristics, using a depth
;;mediated monothetic technique on binary variables .  The data is scanned to identify the most
;;centrally located  variable, which is used to split the data into two groups (TRUE and FALSE
;;grouping). The program then  proceeds by locating the most centrally located variable in each
;;of the subgroups and resplitting the  subgroups. This process is repeated until the required
;;depth has been reached.


;;************************************************************** DEFINITIONS SECTION
.definitions
.define both as integer 4
.define neither as integer 4
.define tf as integer 4
.define ft as integer 4
.define similar as integer 8
.define diff as integer 8
.define score as integer 8
.define prime as text 10
.define secondary as text 10
.define primetot as integer 12
.define primefields as integer 2
.define splitno as integer 1
.define currentnode as text 5
.define mononame as text 15
.define splitvar as text 5
.define fullvar as text 15
.define currentnode as text 5
.define currentlevel as integer 2
.define vircode as text 12
.define recount as integer 4
;;*************************************************************************INTRO SECTION
.reformat off                          ;;switch off formatting to retain columns in output
.let splitno=0                         ;;initialise split counter
.let primetot=0                        ;;initialise prime score accumulator
.let primefields=0                     ;;initialise primefield counter
.open MONOFLDS index SYS:RECORD        ;;open and use order of entry
.gosub initvircodes                    ;;initialise VIRBIN CODES to "1"
.open NODEVARS
.gosub initnodes                       ;;reset NODEVARS transient data for new classification run
.read NODEVARS first not NODEPASSED    ;;preread to trap empty NODEVARS
;;************************************************************** PROCESSING SECTION
.while NODEVARS.SYS:RECORD<>0    ;; START ORDERING PASSES LOOP
.let currentnode=NODEVARS.NODENAME
.let currentlevel=NODEVARS.NODELEVEL
.status Comparing variables for [currentnode] ... [prime] & [secondary]  ;; display progress message
.let splitno=splitno+1                                                   ;;  increment split/pass counter
.gosub initmono
.read MONOFLDS first
.let mononame="NODEVARS."&-MONOFLDS.FLDNAME  ;; create indirect address for first variable
.while MONOFLDS.SYS:RECORD<>0;;START MONOFLDS INITIALISATION LOOP - for each variable
.if [mononame]                         ;; in MONOFLDS , check  NODEVARS to ascertain if
.let MONOFLDS.ORDERED=his bYES          ;;  variable has been previously used to carry out a
.update MONOFLDS                       ;;  split in this branch.. If so, flag in MONOFLDS to bar
.endif                                 ;;  reuse during the commencing pass.
```

```
.read MONOFLDS next
.let mononame="NODEVARS."&-MONOFLDS.FLDNAME     ;; update indirect address for next variable
.endwhile                                       ;; END MONOFLDS INITIALISATION LOOP
.read MONOFLDS first not MONOFLDS.ORDERED       ;; find first candidate prime fieldname
.while MONOFLDS.SYS:RECORD<>0                   ;; START PRIME LOOP - use each fieldname as prime
.let MONOFLDS.CURRENT=YES                       ;; flag it as being used
.update MONOFLDS                                ;; update database with prime flag
.let prime=MONOFLDS.FLDNAME                     ;; store name of prime for use in processing
.read MONOFLDS first not (CURRENT or ORDERED)   ;; set first available non-prime field as secondary
MONOTHETIC EVALUATION:  Prime field [prime] with:
Secondary  Similar  Dissimilar  Difference  R/T Score
.while MONOFLDS.SYS:RECORD<>0                   ;; START SECONDARY LOOP
.let secondary=MONOFLDS.FLDNAME                 ;; set secondary for primary
.read VIRBIN first VIRBIN.CODE=currentnode      ;; position to first record
.gosub initsec                                  ;; zero counters for each new secondary
.while VIRBIN.SYS:RECORD<>0                     ;; START VIRBIN LOOP process all virus records
.gosub compare_current                          ;; determine similarity level for current prime &
.read VIRBIN next VIRBIN.CODE=currentnode       ;; secondary and read next virus record
.endwhile                                       ;; END VIRBIN LOOP
.gosub result                                   ;; print results for pair just analysed
.read MONOFLDS next not (CURRENT or ORDERED)    ;; find next non-prime field for next sec.
.endwhile                                       ;; END SECONDARY LOOP
```

```
.gosub nextprime
.endwhile                                       ;; END PRIME LOOP
.gosub split
.gosub initprime
.read MONOFLDS first MONOFLDS.CURRENT           ;; find current prime field
.let MONOFLDS.CURRENT=NO                        ;; unflag it
.update MONOFLDS
.read MONOFLDS first MONOFLDS.SPLITORDER=splitno ;; find the latest split field again
.let splitvar=MONOFLDS.FLDNAME                  ;; & extract the variable name used

DIVISION FIELD FOR NODE [nodename{5}], LEVEL [nodelevel{3}] IS: [splitvar]
```

```
.gosub updatenodes                              ;; update current & child node information
.gosub updatevircodes                           ;; update node CODEs in VIRBIN for next node
.read NODEVARS first not NODEPASSED             ;; read next NODE not already processed
.endwhile                                       ;; END NODEVARS LOOP
;;**********************************************************************SUBROUTINES SECTION
.subroutines
.label both             ;; BOTH - prime and secondary both true
.let both=both+1
.return
.label neither          ;; NEITHER - neither prime nor secondary true
.let neither=neither+1
.return
.label tf               ;; TF - prime true, secondary false
.let tf=tf+1
.return
.label ft               ;; FT - prime false, secondary true
.let ft=ft+1
.return
.label initsec          ;; INITSEC - initialise counters for each new secondary
.let both=0
.let neither=0
.let tf=0
.let ft=0
.let score=0
.let similar=0
.let diff=0
.return
```

```
.label result                ;;RESULT - calculate & display results
.let similar=@sum(both*neither)
.let diff=@sum(tf*ft)
.let score = @abs(similar-diff)
.let primetot=primetot+score                    ;;increment running score for prime field
[secondary  ] [similar{8}] [diff{8}  ] [score{8}] [primetot{8}]
.return
.label split                 ;;SPLIT - find maximum score for this pass and award ORDER
.status Updating SPLITORDER & ORDERED flag
.sql connect hugh@monoflds
.sql UPDATE monoflds SET splitorder = :splitno WHERE comp_score=(SELECT MAX(comp_score) FROM
monoflds)
.sql UPDATE monoflds SET ordered = YES WHERE comp_score=(SELECT MAX(comp_score) FROM
monoflds)
.return
.label initprime             ;;INITPRIME - reset scores, used flags for all fields before next pass
.status Rezeroing MONOFLDS scores & used flags for next pass ...
.let primefields=0
.read MONOFLDS first
.while MONOFLDS.SYS:RECORD<>0
.let MONOFLDS.COMP_SCORE=0                      ;;zero all COMP_SCOREs & USED flags
.let MONOFLDS.USED=NO                           ;;including prime fields
.update MONOFLDS                                ;;already used
.read MONOFLDS next
.endwhile
.status
.return
.label initmono              ;;INITMONO - reset all ordering information for a new classification
.status Reinitialising SPLIT_ORDER, ORDERED flags for new classification ...
.read MONOFLDS first
.while MONOFLDS.SYS:RECORD<>0
.let MONOFLDS.SPLITORDER=0                      ;;zero SPLIT_ORDERS & ORDERED flags
.let MONOFLDS.ORDERED=NO                        ;;for all MONOFLDS records
.let MONOFLDS.COMP_SCORE=0
.update MONOFLDS
.read MONOFLDS next
.endwhile
.status
.return
.label nextprime             ;; NEXTPRIME - change prime field to next available variable
.read MONOFLDS first MONOFLDS.CURRENT    ;;find current prime field
.let MONOFLDS.COMP_SCORE=PRIMETOT        ;;store final score for prime field
.let MONOFLDS.CURRENT=NO                 ;;reset current prime to non-prime
.let MONOFLDS.USED=YES                   ;;flag ex-prime as used for this pass
.update MONOFLDS                         ;;save to database
.let primetot=0                          ;;re-initialise for next prime field
.read MONOFLDS next not (USED or ORDERED)  ;;find next candidate prime fieldname
.let primefields=primefields+1           ;;increment number of primes used
.return
.label compare_current       ;; COMPARE_CURRENT - establish similarity level for
.if [prime]                              ;; current record prime/secondary field combination
.if [secondary]                          ;; and update relevant counters
.gosub both                              ;; both PRIME and SECONDARY are true
.endif
.endif
.if [prime]
.else
.if [secondary]
.else
.gosub neither                           ;; neither PRIME or SECONDARY are true
.endif                                   ;; indirection syntax requires use of 'else ' clause to serve
.endif                                   ;; as negation of negated branch condition
.if [prime]
```

```
.if [secondary]
.else
.gosub tf                              ;; PRIME is true, but SECONDARY is false
.endif
.endif
.if [prime]
.else
.if [secondary]
.gosub ft                              ;; SECONDARY is true, but PRIME is false
.endif
.endif
.return
.label initnodes            ;;INITNODES - reset all NODEVAR variables for
.status Initialising NODEVARS records.... ;; new classification
.read NODEVARS first                   ;; for all depth control database records, zero variable values.
.while NODEVARS.SYS:RECORD<>0
.let NODEVARS.EXE=NO
.let NODEVARS.COM=NO
.let NODEVARS.RES=NO
.let NODEVARS.MBR=NO
.let NODEVARS.PSITE=NO
.let NODEVARS.O_W=NO
.let NODEVARS.CMD=NO
.let NODEVARS.NODEPASSED=NO
.let NODEVARS.FILTER=""
.update NODEVARS
.read NODEVARS next
.endwhile
.status
.return
.label initvircodes             ;;INITVIRCODES - set all VIRBIN record codes to
.let recount=0                                  ;; read "1" (root node)
.status Initialising VIRBIN CODES .....         ;; display progress message in status line
.read VIRBIN first
.while recount<VIRBIN.SYS:NUMREC                ;; while processed records less than total records,
.let VIRBIN.CODE="1"                            ;; initialise each record's CODE field
.update VIRBIN                                  ;; with starting point for new classification run.
.read VIRBIN next
.let recount=recount+1
.endwhile
.status
.return
.label updatenodes ;;UPDATENODES - mark current node used, current & child VARS & FILTER
.let fullvar="NODEVARS."&-splitvar      ;;START NODEVARS update process
.read NODEVARS first @substr(NODENAME,1,currentlevel)=@substr(currentnode,1,currentlevel)
.let NODEVARS.NODEPASSED=YES    ;; update NODEVAR information for current
.while NODEVARS.SYS:RECORD<>0    ;; do for all records in NODEVARS
.let [fullvar]=YES                      ;; node and child nodes to indicate use of current
.if splitno=1                           ;; variable and add variable name to filter paths
.let NODEVARS.FILTER=@TRIM(NODEVARS.FILTER)&-splitvar
.else
.let NODEVARS.FILTER=@TRIM(NODEVARS.FILTER)&", "&-splitvar
.endif
.update NODEVARS
.read NODEVARS next @substr(NODENAME,1,currentlevel)=@substr(currentnode,1,currentlevel)
.endwhile                               ;;END NODEVARS update process
.return
.label updatevircodes       ;;UPDATEVIRCODES - for all VIRBIN records for currentnode,
.status Updating VIRBIN CODES .....     ;;display progress message in status line,
.let vircode="VIRBIN."&-splitvar        ;; concatenate indirect address for variable's fieldname,
.read VIRBIN first VIRBIN.CODE=currentnode  ;; establish whether virus is in Y or N category
.while VIRBIN.SYS:RECORD<>0             ;; for the split variable used, and
.if [vircode]                           ;; update CODE accordingly.
```

```
.let VIRBIN.CODE=@TRIM(VIRBIN.CODE)&-"Y"
.else
.let VIRBIN.CODE=@TRIM(VIRBIN.CODE)&-"N"
.endif
.update VIRBIN
.read VIRBIN next VIRBIN.CODE=currentnode
.endwhile
.status
.return
;;*****************************************
;;*****************************************
;;*****************************************
```

APPENDIX F - Display of processing progress

MONOTHETIC EVALUATION: ***Prime field*** **EXE** ***with:***

Secondary	Similar	Dissimilar	Difference	R/T Score
RES	46754	17724	29030	29030
COM	13122	28782	15660	44690
MBR	2618	9858	7240	51930
PSITE	22120	14670	7450	59380
O_W	11049	7104	3945	63325
CMD	20460	44960	24500	87825

MONOTHETIC EVALUATION: ***Prime field*** **RES** ***with:***

Secondary	Similar	Dissimilar	Difference	R/T Score
EXE	46754	17724	29030	29030
COM	16245	21203	4958	33988
MBR	9936	832	9104	43092
PSITE	22833	14235	8598	51690
O_W	1386	20962	19576	71266
CMD	22528	37240	14712	85978

MONOTHETIC EVALUATION: ***Prime field*** **COM** ***with:***

Secondary	Similar	Dissimilar	Difference	R/T Score
EXE	13122	28782	15660	15660
RES	16245	21203	4958	20618
MBR	735	18197	17462	38080
PSITE	35979	3933	32046	70126
O_W	5250	6072	822	70948
CMD	58344	608	57736	128684

MONOTHETIC EVALUATION: ***Prime field*** **MBR** ***with:***

Secondary	Similar	Dissimilar	Difference	R/T Score
EXE	2618	9858	7240	7240
RES	9936	832	9104	16344
COM	735	18197	17462	33806
PSITE	651	18569	17918	51724
O_W	0	2014	2014	53738
CMD	1255	14553	13298	67036

MONOTHETIC EVALUATION: ***Prime field*** **PSITE** ***with:***

Secondary	Similar	Dissimilar	Difference	R/T Score
EXE	22120	14670	7450	7450
RES	22833	14235	8598	16048
COM	35979	3933	32046	48094
MBR	651	18569	17918	66012
O_W	222	30150	29928	95940
CMD	32643	8729	23914	119854

MONOTHETIC EVALUATION: ***Prime field*** **O_W** ***with:***

Secondary	Similar	Dissimilar	Difference	R/T Score
EXE	11049	7104	3945	3945
RES	1386	20962	19576	23521
COM	5250	6072	822	24343
MBR	0	2014	2014	26357
PSITE	222	30150	29928	56285
CMD	9916	6544	3372	59657

MONOTHETIC EVALUATION: ***Prime field*** **CMD** ***with:***

Secondary	Similar	Dissimilar	Difference	R/T Score
EXE	20460	44960	24500	24500
RES	22528	37240	14712	39212
COM	58344	608	57736	96948
MBR	1255	14553	13298	110246
PSITE	32643	8729	23914	134160
O_W	9916	6544	3372	137532

DIVISION FIELD FOR NODE 1 , LEVEL 1 IS: CMD

MONOTHETIC EVALUATION: ***Prime field*** **EXE** ***with:***

Secondary	Similar	Dissimilar	Difference	R/T Score
RES	20150	4410	15740	15740
COM	326	558	232	15972
MBR	1120	161	959	16931
PSITE	3168	5439	2271	19202
O_W	4437	2960	1477	20679

MONOTHETIC EVALUATION: ***Prime field*** **RES** ***with:***

Secondary	Similar	Dissimilar	Difference	R/T Score
EXE	20150	4410	15740	15740
COM	253	567	314	16054
MBR	950	0	950	17004
PSITE	7840	1738	6102	23106
O_W	790	8032	7242	30348

MONOTHETIC EVALUATION: ***Prime field*** **COM** ***with:***

Secondary	Similar	Dissimilar	Difference	R/T Score
EXE	326	558	232	232
RES	253	567	314	546
MBR	20	0	20	566
PSITE	400	126	274	840
O_W	108	406	298	1138

MONOTHETIC EVALUATION: ***Prime field*** **MBR** ***with:***

Secondary	Similar	Dissimilar	Difference	R/T Score
EXE	1120	161	959	959

RES	950	0	950	1909
COM	20	0	20	1929
PSITE	123	800	677	2606
O_W	0	185	185	2791

MONOTHETIC EVALUATION: ***Prime field*** **PSITE** ***with:***

Secondary	Similar	Dissimilar	Difference	R/T Score
EXE	3168	5439	2271	2271
RES	7840	1738	6102	8373
COM	400	126	274	8647
MBR	123	800	677	9324
O_W	16	14035	14019	23343

MONOTHETIC EVALUATION: ***Prime field*** **O_W** ***with:***

Secondary	Similar	Dissimilar	Difference	R/T Score
EXE	4437	2960	1477	1477
RES	790	8032	7242	8719
COM	108	406	298	9017
MBR	0	185	185	9202
PSITE	16	14035	14019	23221

DIVISION FIELD FOR NODE 1Y , LEVEL 2 IS: RES

MONOTHETIC EVALUATION: ***Prime field*** **EXE** ***with:***

Secondary	Similar	Dissimilar	Difference	R/T Score
RES	4329	4165	164	164
COM	4160	5760	1600	1764
MBR	282	4710	4428	6192
PSITE	7752	1608	6144	12336
O_W	1440	592	848	13184

MONOTHETIC EVALUATION: ***Prime field*** **RES** ***with:***

Secondary	Similar	Dissimilar	Difference	R/T Score
EXE	4329	4165	164	164
COM	4752	3872	880	1044
MBR	2666	330	2336	3380
PSITE	3834	3294	540	3920
O_W	73	2925	2852	6772

MONOTHETIC EVALUATION: ***Prime field*** **COM** ***with:***

Secondary	Similar	Dissimilar	Difference	R/T Score
EXE	4160	5760	1600	1600
RES	4752	3872	880	2480
MBR	202	4650	4448	6928
PSITE	9042	990	8052	14980
O_W	732	1460	728	15708

MONOTHETIC EVALUATION: ***Prime field*** **MBR** ***with:***

Secondary	Similar	Dissimilar	Difference	R/T Score
EXE	282	4710	4428	4428
RES	2666	330	2336	6764
COM	202	4650	4448	11212
PSITE	208	5771	5563	16775
O_W	0	528	528	17303

MONOTHETIC EVALUATION: ***Prime field*** **PSITE** ***with:***

Secondary	Similar	Dissimilar	Difference	R/T Score
EXE	7752	1608	6144	6144
RES	3834	3294	540	6684
COM	9042	990	8052	14736
MBR	208	5771	5563	20299
O_W	66	3030	2964	23263

MONOTHETIC EVALUATION: ***Prime field*** **O_W** ***with:***

Secondary	Similar	Dissimilar	Difference	R/T Score
EXE	1440	592	848	848
RES	73	2925	2852	3700
COM	732	1460	728	4428
MBR	0	528	528	4956
PSITE	66	3030	2964	7920

DIVISION FIELD FOR NODE 1N , LEVEL 2 IS: PSITE

MONOTHETIC EVALUATION: ***Prime field*** **EXE** ***with:***

Secondary	Similar	Dissimilar	Difference	R/T Score
COM	258	124	134	134
MBR	500	126	374	508
PSITE	620	726	106	614
O_W	122	516	394	1008

MONOTHETIC EVALUATION: ***Prime field*** **COM** ***with:***

Secondary	Similar	Dissimilar	Difference	R/T Score
EXE	258	124	134	134
MBR	15	0	15	149
PSITE	243	20	223	372
O_W	8	249	241	613

MONOTHETIC EVALUATION: ***Prime field*** **MBR** ***with:***

Secondary	Similar	Dissimilar	Difference	R/T Score
EXE	500	126	374	374
COM	15	0	15	389
PSITE	27	484	457	846
O_W	0	25	25	871

MONOTHETIC EVALUATION: ***Prime field*** **PSITE** ***with:***

Secondary	Similar	Dissimilar	Difference	R/T Score

EXE	620	726	106	106
COM	243	20	223	329
MBR	27	484	457	786
O_W	0	1225	1225	2011

MONOTHETIC EVALUATION: ***Prime field*** **O_W** ***with:***

Secondary	Similar	Dissimilar	Difference	R/T Score
EXE	122	516	394	394
COM	8	249	241	635
MBR	0	25	25	660
PSITE	0	1225	1225	1885

DIVISION FIELD FOR NODE 1YY , LEVEL 3 IS: PSITE

MONOTHETIC EVALUATION: ***Prime field*** **EXE** ***with:***

Secondary	Similar	Dissimilar	Difference	R/T Score
COM	0	155	155	155
MBR	0	0	0	155
PSITE	340	2070	1730	1885
O_W	2224	304	1920	3805

MONOTHETIC EVALUATION: ***Prime field*** **COM** ***with:***

Secondary	Similar	Dissimilar	Difference	R/T Score
EXE	0	155	155	155
MBR	0	0	0	155
PSITE	0	32	32	187
O_W	32	0	32	219

MONOTHETIC EVALUATION: ***Prime field*** **MBR** ***with:***

Secondary	Similar	Dissimilar	Difference	R/T Score
EXE	0	0	0	0
COM	0	0	0	0
PSITE	0	0	0	0
O_W	0	0	0	0

MONOTHETIC EVALUATION: ***Prime field*** **PSITE** ***with:***

Secondary	Similar	Dissimilar	Difference	R/T Score
EXE	340	2070	1730	1730
COM	0	32	32	1762
MBR	0	0	0	1762
O_W	4	4680	4676	6438

MONOTHETIC EVALUATION: ***Prime field*** **O_W** ***with:***

Secondary	Similar	Dissimilar	Difference	R/T Score
EXE	2224	304	1920	1920
COM	32	0	32	1952
MBR	0	0	0	1952
PSITE	4	4680	4676	6628

DIVISION FIELD FOR NODE 1YN , LEVEL 3 IS: O_W

MONOTHETIC EVALUATION: *Prime field* **EXE** *with:*

Secondary	Similar	Dissimilar	Difference	R/T Score
RES	3150	1147	2003	2003
COM	71	4290	4219	6222
MBR	198	133	65	6287
O_W	0	136	136	6423

MONOTHETIC EVALUATION: *Prime field* **RES** *with:*

Secondary	Similar	Dissimilar	Difference	R/T Score
EXE	3150	1147	2003	2003
COM	2652	1400	1252	3255
MBR	180	139	41	3296
O_W	0	142	142	3438

MONOTHETIC EVALUATION: *Prime field* **COM** *with:*

Secondary	Similar	Dissimilar	Difference	R/T Score
EXE	71	4290	4219	4219
RES	2652	1400	1252	5471
MBR	128	270	142	5613
O_W	66	0	66	5679

MONOTHETIC EVALUATION: *Prime field* **MBR** *with:*

Secondary	Similar	Dissimilar	Difference	R/T Score
EXE	198	133	65	65
RES	180	139	41	106
COM	128	270	142	248
O_W	0	4	4	252

MONOTHETIC EVALUATION: *Prime field* **O_W** *with:*

Secondary	Similar	Dissimilar	Difference	R/T Score
EXE	0	136	136	136
RES	0	142	142	278
COM	66	0	66	344
MBR	0	4	4	348

DIVISION FIELD FOR NODE 1NY , LEVEL 3 IS: EXE

MONOTHETIC EVALUATION: *Prime field* **EXE** *with:*

Secondary	Similar	Dissimilar	Difference	R/T Score
RES	54	864	810	810
COM	459	90	369	1179
MBR	0	696	696	1875
O_W	648	36	612	2487

MONOTHETIC EVALUATION: *Prime field* **RES** *with:*

Secondary	Similar	Dissimilar	Difference	R/T Score
EXE	54	864	810	810
COM	108	432	324	1134
MBR	728	26	702	1836
O_W	13	742	729	2565

MONOTHETIC EVALUATION: *Prime field* **COM** *with:*

Secondary	Similar	Dissimilar	Difference	R/T Score
EXE	459	90	369	369
RES	108	432	324	693
MBR	0	435	435	1128
O_W	280	100	180	1308

MONOTHETIC EVALUATION: *Prime field* **MBR** *with:*

Secondary	Similar	Dissimilar	Difference	R/T Score
EXE	0	696	696	696
RES	728	26	702	1398
COM	0	435	435	1833
O_W	0	435	435	2268

MONOTHETIC EVALUATION: *Prime field* **O_W** *with:*

Secondary	Similar	Dissimilar	Difference	R/T Score
EXE	648	36	612	612
RES	13	742	729	1341
COM	280	100	180	1521
MBR	0	435	435	1956

DIVISION FIELD FOR NODE 1NN , LEVEL 3 IS: RES