OVERVIEW

THE WINDS OF CHANGE: UP-DATES TO THE EICAR TEST FILE

Eddy Willems
Data Alert International, Belgium
EICAR Director Information and Press

In 1991 the inaugural meeting of the European Institute for Computer Anti-Virus Research (now better known as EICAR) took place in Brussels. A few years later, as the result of cooperative effort between a number of anti-virus researchers, the EICAR standard anti-virus test file was created in order to provide an industry standard solution for a number of common questions – the test file remained unchanged until May 2003.

WHAT IS THE EICAR TEST FILE?

The purpose of the EICAR test file is to provide an industry standard solution for the following questions:

- Is my anti-virus program installed correctly – that is, does it intercept and/or detect viruses as it is supposed to?
- What happens when my anti-virus program detects a virus?
- Which messages are displayed?
- What about 'custom warnings', batch files and system admin notifications over the network?

The idea is that anti-virus programs detect the test file exactly as they would detect a virus, and effectively treat it as a virus.

Of course, a custom file for each anti-virus program would serve the same purpose, but the standard test file is intended to simplify the testing process – in particular in cases where multiple products are being tested and evaluated. The anti-virus industry adapted their products to the EICAR test file very well.

The following is a short abstract from the original EICAR test file definition:

> The file is a legitimate DOS program, and produces sensible results when run (it prints the message 'EICAR-STANDARD-ANTIVIRUS-TEST-FILE'). It is also short and simple – in fact, it consists entirely of printable ASCII characters, so that it can easily be created with a

regular text editor. Any anti-virus product that supports the test file should detect it in any file providing that the file starts with the following 68 characters:

X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

To keep things simple, the file uses only upper case letters, digits and punctuation marks, and does not include spaces. The only thing to watch out for when typing in the test file is that the third character is the capital letter 'O', not the digit zero.

The string should be saved to a file with a .COM extension (EICAR.COM being the most obvious choice). So, when it is run, it will display the string 'EICAR-STANDARD-ANTIVIRUS-TEST-FILE!'.

As a side note, the file is printable so that it can easily be printed in a manual, included in software documentation, dictated over the telephone, or sent by fax.

It is not recommended that the EICAR file be included as a 'standalone' file in the anti-virus package in 'binary form', as users might run the anti-virus program on the package before realising what the test file is for.

The complete definition of the EICAR test file can be found at http://www.eicar.org/anti_virus_test_file.htm.

BAT/BWG.A@MM

In May 2002 the MS DOS batch worm Bat/Bwg.a@MM appeared. This worm was generated using a virus construction kit called Bwg ('Batch worm generator'). To date, this virus has not been seen in the wild.

The virus arrives as an email attachment, b.bat. Using *Outlook*, the virus will send an email to all recipients in the address book. When the attachment is double-clicked, the virus drops several copies of itself:

C:\a.bat C:\pro\a.jpg.bat

C:\b.bat %Windir%\b.arv.bat

Then it drops a VBS script, c:\dkhcz.vbs, which contains the code needed to mass-mail the virus.

The virus checks whether *mIRC* or *pIRCch* is installed on the machine. The worm will edit *mIRC*'s script.ini to send the file C:\pro\a.jpg.bat and drops b.arv.bat into the Windows directory. If *pIRCch* is installed the virus modifies events.ini to send b.arv.bat.

The virus can infect %windir%\startm~1\progra~1\autost~1*.bat and drop %windir%\Start Menu\Programs\StartUp\bjits.bat. In addition, it can copy itself to %windir%\Desktop*.ifk and rename %windir%\Desktop*.ifk to *.bat.

THE PROBLEM

The most significant feature of Bat/Bwg.a@MM is the fact that it is an attack on the EICAR test file. The virus starts with the EICAR string, which means that when it is run, a 'File not found' error is generated, but the execution of the virus continues.

A large number of anti-virus products misdetected this virus as the EICAR test file when it first appeared. This resulted in a lot of debate on various anti-virus discussion forums. Some members of the anti-virus community advocated changing the test file completely. After a while, each anti-virus vendor worked out their own way for their products to detect the EICAR test file properly.

THE CHANGE: TAKE ONE

The members of EICAR observed the problems that had arisen as a result of Bat/Bwg.a@MM and wanted to help the anti-virus vendors by changing the definition of the test file *slightly*, so that EICAR would have a fully correct and safe definition in use.

After consulting a number of anti-virus experts EICAR proposed the following change to the file:

The file is a legitimate DOS program, and produces sensible results when run (it prints the message 'EICAR-STANDARD-ANTIVIRUS-TEST-FILE'). It is also short and simple – in fact, it consists entirely of printable ASCII characters, so that it can easily be created with a regular text editor. Any anti-virus product that supports the test file should detect it in any file providing that the file starts with the following 68 characters, **and is exactly 68 bytes long:**

X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

To keep things simple …

However, this proposal provoked some strong, negative response from members of the anti-virus industry – most anti-virus experts felt that the definition was neither explicit nor exact enough. Again, a lot of discussion took place on various anti-virus forums and even at WildList and CARO meetings.

THE CHANGE: TAKE TWO

EICAR decided to change the file again, in such a way that we would have mutual agreement between most anti-virus vendors. In order to achieve agreement, several anti-virus experts were asked for their input.

Responses were gathered from more than 40 members of the anti-virus industry. Afterwards I tried to combine all the

ideas into the latest definition change which was published 1 May 2003 on the EICAR website:

> The file is a legitimate DOS program, and produces sensible results when run (it prints the message 'EICAR-STANDARD-ANTIVIRUS-TEST-FILE'). It is also short and simple – in fact, it consists entirely of printable ASCII characters, so that it can easily be created with a regular text editor. Any anti-virus product that supports the test file should detect it in any file providing that the file starts with the following 68 characters:
>
> X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
>
> **The first 68 characters is the known string. It may be optionally appended by any combination of whitespace characters with the total file length not exceeding 128 characters. The only whitespace characters allowed are the space character, tab, LF, CR, CTRL-Z.**
>
> To keep things simple …

The new definition was sent to the various anti-virus forums at the beginning of this year in order to give every anti-virus vendor sufficient time to prepare for the necessary changes within their documents or programs.

To date, we have received no new reactions to or additional comments about the latest definition from members of the anti-virus industry.

In fact, one advantage of the 'new' test file is that it is not a complete change to the file. It is only the test file *definition* that has been narrowed in order to make it impossible to use the EICAR test file in a malicious way. This means that the majority of detection mechanisms within anti-virus programs do not need to be changed.

THE LAST WORD

I am certain that this will not be the last word concerning the EICAR test file.

During this year's EICAR conference (see this issue p.13) I presented an FAQ list concerning the file. Why not create different test files to test the other functionalities of the programs? Why not create a file to test for VBS viruses, macro viruses or blended threats? These questions were raised, but reach far beyond the original purpose of the file and we don't want to touch it in that way. The complete FAQ list will be available on the EICAR website shortly (see http://www.eicar.org/). I am happy to hear other suggestions about the test file, providing they are reasonable and that we are able to meet the needs of all anti-virus vendors. Any comments or suggestions should be sent to press@eicar.org.