Metaviruses

Metaviruses
by Meza
[February 2000]

I want to speak of a topic that has been put into use recently , and that , I am sure , will become highly wide-spread in the future - downloading virus additions from the internet.

Why is this necessary and how is it possible?

To answer to first question is easy. Firstly , because it is possible to download to infected computer as much as you want , we can no longer worry about the size of the code. Secondly , updates can be of two types - updates of the whole body of the virus , or an extension module. The virus is changed in the first case by a similar , but with a different signature , or in general by another virus , making finding the virus by antivirus programs more difficult. In the second case , an extension module can be an infector for other types of files , or something more specific : keyloger/password sender or a backdoor .So viruses , except duplications , will be able to do some usefull work towards what , in my opinion , is revolutionary step in virus evolution . Or you can imagine the determination of antivirus software on an infected computer , by downloading a targeted anti-antivirus module! Thus we get a new level of adaptation for viruses. It is possible even to name these modules by genes that must lead amateurs to think of the genetic models of viruses. It is possible to go further and visualize communities of viruses , each of which , being on infected computers , download from the internet other "friend" viruses. Spreading of such a virus would be so fast , like such known rabbits as Melissa :)

Now about realization of this. The first thing that is required - the corresponding architecture of the virus. Obviously this virus must be made up of a server part , which , being completely resident , has charge of searching for , delivery and execution of the additions. Thus , in infected file , regardless of the type , there must be two part : the loader and the server itself - dual architecture. The loader throws the server onto disk and starts itself, and then sends control back to the victim. The server must have in itself a procedure to scan the disk and infect at least one type of file (think yourselves why). So after changing most of the server with an update , all following generations will be new , with a different signature , or possibly with another algorithm .Here it is necessary to say that when the loader starts the server , it must did not switch the new version of the server with the older one from the previous generation. The modules can be dlls , interfaces can be different. Scanning of the disk is

possible to do from the server i.e. a targeted extension module (for determined type of files) must only export the infection procedure. BUT! It must infect with the respective loader and the CURRENT server !

Now we are ready to address the most complex question - where to hold the additions? There are several possibilities. First , and simplest - a fixed url. This is so simple , it is not nessesary to speak about. But , certainly , this scheme will not work for a long time - as soon as avers have got your virus in their own bloodthirsty :) hands they will close this site. And now your baby will remain alone in this cruel world! It will be able to replicate , but it will be old wave of virus .
I have thought for a couple of days , and have found a more beautiful option - to use the search engines, like yahoo.com . The virus in such a case knows the key phrase and search server. It's your problem to upload the additions on some site and add its url to the base of the search server. Even though page will be closed , you may open a new one and register it on the search engine! On a whole it is that! At first , I liked this idea very much ; good protection from avers and feds and easy enough to code... But the world is so hard !:) This method has the weak spot too - if the virus would become known enough , avers can set a filter for your key phrase in the search engine .

Another variation on the previous method is the use of a ftp search engine , here it is possible to simply assign a filename and search for it on ftp servers , which mostly are public i.e. anyone can upload to them. You may ask , but how does this method differ from previous? The difference is radical!! Anyone can upload!! I.e. even your virus!! Thereby it is possible to organize migrating of base of modules (though not updated) . For instance , a virus counts out the generations , and at achievement of some number , it searches for some wide-spread file , to get a list of ftp-servers. Amongst them it searches for public , uploads there all that it has , under NEW names, but in the future generations prescribes THESE name! A beautiful picture , isn't it?:) Hope avers will like these ideas...:) The minus is the same - a filter on the search engine...But in this instance it is harder to do - too many filters to put in the case of many generations. Apropos , while I wrote this I thought of a new idea! After all , avers can not check ALL versions of a virus i.e if a migration has occurred of the base of modules , new generations are already protected from them !! Yes , you will say , i too do not know where and under what names all this stuff lies! Yes and no - I will answer!! It is possible to organize feedback - viruses can email , for instance , to you all the necessary info :). Certainly , it is necessary to change the email address too...Already in the progress of writing this article I thought of another excellent improvement of this method. Visualize a command interpreter in a virus, which reads the commands from a file , which lies on ftp. In this case you can prescribe any variantion of update. So here , move only this batch file ; its location is sent to you through an additional communication channel , and later you can edit this file. So avers must have a copy of virus from EACH generation to be sure that they know everything about all generations! Certainly , this is not absolute protection too, but if you think a bit, you will understand that to catch such viruses is very hard.

And, at last, apotheosis of the inflamed imagination - instant messaging systems , like ICQ, AIM, and also IRC. The implementation is a little bit more difficult, but is quite real and possible, especially in the latter case. The size - believe me, a few kb in all! But you get FULL interactivity!!! Simply a fairy tale... Imagine viruses of miscellaneous writers sitting on a channel and exchanging modules!!! An avers nightmare !:) The problems - the same , you can not simply prescribe in a virus the name of a channel for IRC or a UIN for ICQ , coz it easy for avers to find! But the solution is the same as I offered for the previous method. For instance , the same server can , after a certain number of generations , generate a new name for the channel or register a new UIN for interaction with its master and report it to you. As it is , it is possible to apply encoding with public keys, so even if avers get the letter with the new properties , they do not find out anything and it would be rather useful to apply a digital signature in all the downloads by your virus from the inet.
As you can see, you have the choice. But the most difficult thing, personally , is to select the best method..:)
Another thing that I want to note. The avers update their products too . And they do not have a problem with where to hold updates. BUT! They can not control the time of the update- that all depends on the user. And I have seen computers, on which there was an anti-virus and BO (Back Orifice), FIRST version!!! I.e. BO, which is already known for about two years now, which is detected by everything, almost by the calculator (calc.exe:))!!! Whether these users don't know at all about updating, whether they consider it enough to install an anti-virus on their computer and the viruses will be afraid !:) So in opposition to avers , the virus is updated by itself and can do it though each day! Shall we miss such advantage?!

In summary I want to say, that the writing of such virus is a difficult task. But I am sure that there are people capable of realising it, alone or together. As I say, that in my view, this article confirms this also, that viruses becoming more complicated also concludes that there is more and more of an application for a high-level language in writing a virus, for example ?/? ++, but it already subject of another article!:)

The combination of modern ways of mutation in viruses and mutation through network updates, in my view, demonstrates that first if it will not die, it will remain only by auxiliary means. And in the scene there will be viruses of a new generation - metaviruses! And they radically differ from old viruses! Metavirus are dynamic frames of modules, different functions, but integrated by for purpose. And the purpose is this - the survival of frame as a whole and serving its master! One metavirus from one generation can differ absolutely from another, except for the master (though also this , at desire can be changed:)) Through updates you can change the signature, target platform (type of the infected file), algorithm, way of communication with the master, function etc. Everything that you can invent can be changed! And now think, what the avers can do to oppose this? Nothing. Only passively wait, when somehow they will receive any generation of metavirus, to find its signature and again to wait... (you may say, what about heuristics? Yes, it is a strong step from their group, but despite it , it is possible to struggle successfully). Why is this scheme so is strong? Because the virus acts not alone but in interaction with the master! Certainly , this requires some

efforts from the master , but for all these things, it is a nessecary sacrifice to make. An absolutely independent metavirus is possible only when artificial intelligence is fully availabile for the task , but I can't do that yet:)

I have written " will leave the scene " and here i have begun to doubt it... The matter of fact, writing metavirus - is more difficult, than to write a usual virus. System approaches here are required already, if it is possible to be expressed so. Only units in the viral world are capable of realising such idea in a individual, and successful group projects in the virus world are not known to me yet. (by the way, metaviruses are more a friend to the group project than the usual virus, coz it consists of several significantly independent parts). Though there is one more variant - a cyberweapon... And where there are weapons, there is also money... But this is in the future..(though we will reach it, I think).

On cause of ideas and offers on this article write on mail meza_vx@yahoo.com

---