FEATURE

The Number of the Beasts

Denis Zenkin
Kaspersky Lab, Russia

As a long-time, regular reader of *Virus Bulletin* I always peruse all the articles and reviews published in the magazine carefully. One of the most interesting parts is the monthly published virus prevalence table. I am very happy to have such statistics. The Prevalence Table is very useful, giving users a snapshot of what is really going on in the virus world. Many people are too lazy (sorry, I should say busy) to look into Joe Wells' WildList to see the most dangerous threats. If they did, they would not see the prevalence of different viruses. On the other hand, *VB's* Prevalence Table is a must for everyone who deals with computers, no matter whether they are a network administrator or a home user.

As an avid *VB* Prevalence Table fan, I decided to see what is behind them and the results are extremely interesting. A summary of all the virus statistics published in *Virus Bulletin* reveals the top ten viruses in history, the top viruses by type and the viruses of the year. This enables one to draw a general chart for the number of infections since 1995, compile an aggregate virus prevalence table for the whole period and prepare a pie-chart of the most prevalent virus types. Finally, we can take a look at the most dangerous systems for computing as regards the number of viruses that could affect them.

Top Ten Viruses in History

W97M/ColdApe is a very sensitive case. As you have probably noticed, the data for this virus was omitted from the Prevalence Table in the February issue and ColdApe was rated as self-reporting.

	Name	Type	No. of Incidents	Percentage
1	ColdApe	Macro	8856	15.3%
2	Cap	Macro	3893	6.7%
3	Class	Macro	3847	6.6%
4	Ethan	Macro	3512	6.1%
5	Win32/Ska	File	3462	6.0%
6	Laroux	Macro	2548	4.4%
7	Marker	Macro	2423	4.2%
8	Win95/CIH	File	2172	3.8%
9	Concept	Macro	2007	3.5%
10	Form	Boot	1517	2.6%

Before this, all ColdApe reports were counted as 'true'. Just imagine, every day an infected computer sent out a message to Nick FitzGerald (the virus's original payload). Each time was counted as a new incident, but actually this is not true. In only one year (1999) it registered 8,622 times, which is unbelievable! This is the reason why it tops our 'Top Ten Viruses' list.

Top Viruses by Virus Types

There is no need to introduce the nominees. All of them are 'well known' due to the great financial loss they caused.

Nomination	Place	Name	Incidents	Percentage
Top macro virus	1	ColdApe	8856	15.3%
Top file virus	8	Win95/CIH	2172	3.8%
Top boot virus	10	Form	1517	2.6%
Top script virus	26	VBS/Kak	660	1.1%
Top worm	5	Win32/Ska	3376	6.0%

Once again, we should be careful when we analyse W97M/ColdApe. If we omit the data for this virus, then the real 'winner' would be the WM/Cap macro virus. With regards to the top script virus, I should mention that things will change. In only one month, VBS/LoveLetter scored 654 incidents, while JS/Kak has been reported 660 times since its discovery in late 1999. Due to a great number of variations, next month we expect LoveLetter to take the lead. It even has the chance to become 'Virus of the Year'.

Viruses of the Year

This table shows how fast things are changing. For many years since the first PC virus was discovered, boot viruses were always the type that spread the most widely.

Year	Name	Incidents (for year)	Percentage (for year)
1995	Form	328	13.3%
1996	Concept	762	15.9%
1997	Cap	694	14.7%
1998	Cap	953	16.8%
1999	ColdApe	8622	25.5%
2000*	Win32/Ska	778	12.1%

After 1995, when the first macro virus – WM/Concept – appeared, it occupied the top position for four years. Only in 2000 (*shown up to May) did worm-style viruses, due to their exceptional mass-mailing abilities, top the list. In 1999, if we omit the 'self-reporting' ColdApe, the top virus would be W97M/Class, with 3216 incidents and 12.6% of the total reports. Nowadays, the Internet has become the main virus propagation source. Thus, to become widespread, the virus requires special worm-style spreading abilities via email, IRC channels and so on. Many more viruses of this type are appearing. For the most part they are still macro, script or file viruses, but they feature new propagation technology.

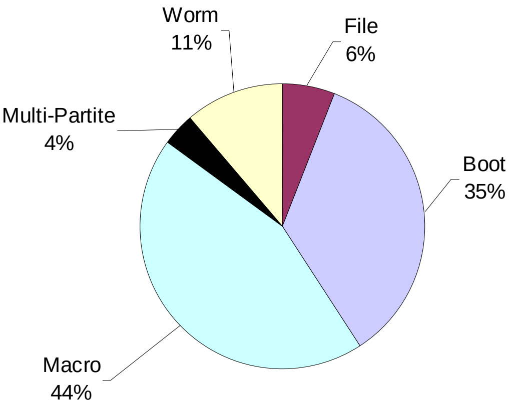

Figure 1: Most prevalent virus types between 1995 and May 2000.

Despite numerous rivals, macro viruses are still number one in the world's virus charts. However, modern trends demonstrate that more and more of them are moving into the worm group and, with each year, the macro part of the pie will become smaller and smaller while the worm section will grow steadily and quickly.

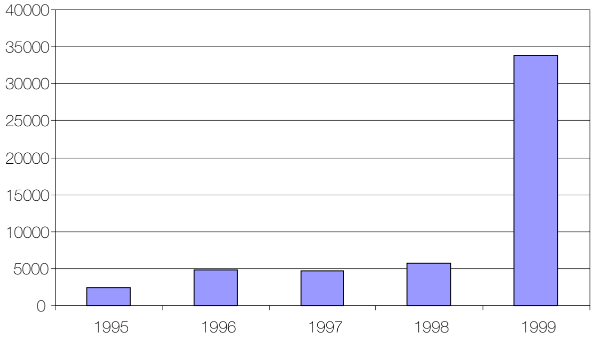

Figure 2: Number of virus incidents (1995–1999)

You would probably be amazed at the enormous virus turnaround in 1999. A closer look reveals that more than 8,000 of a total of 33,830 incidents reported were of ColdApe, which is actually a false representation.

However, even if we omit the ColdApe virus again we can see that 1999 was still the year when the highest number of separate virus incidents were reported. Who knows what will happen this year? Another VBS/LoveLetter epidemic will catapult 2000 into the lead. On the other hand, viruses are just like seasonal workers; it is very hard to predict when they will appear. In any single month the number of virus incidents could double or even triple because of a brand new virus.

VB Prevalence Table figures confirm that macro viruses are losing their dominant position to worm-style viruses. However, the macro viruses still prevail. Together with worms written in script languages, they will be the major threat to both individual and corporate users in the future. There is a reasonable explanation for this. Firstly, it is very easy to develop a macro or script virus. The only thing a virus writer needs to have is a basic knowledge of VBA or VBS programming languages. They are so simple that even a schoolboy could manage this in a couple of weeks. Secondly, these viruses are available as source code. This means other people can easily construct their own viruses by applying the slightest change to the original. Thirdly, these viruses are aimed at the most popular applications, which are used by millions of people worldwide.

Finally, these applications usually have poor protection with many security breaches discovered every month. We are very lucky that virus writers neither pay enough attention to security-related Internet conferences nor seem to have the money to subscribe to *Virus Bulletin*. Otherwise, they would issue a new virus exploiting security breaches each time they are discovered!

It is no secret that nowadays the most dangerous application a user can have is *MS Office* (43.3% of incidents in 2000 occurred on this platform). The problem is that *MS Office* usually runs on an operating system called *Windows*, which is not safe either (29.7% of incidents). By default, *Windows* has a *Scripting Host* installed, which has encountered 26.2% of incidents so far this year. The news would not be that bad if the vast majority of computer users stopped using any of the applications mentioned above. But the harsh truth is they do continue to use them.

I see two ways to alter this state of affairs. The first involves a general migration to alternative operating systems, office and email applications. Even so, it will not save us from viruses from here to eternity. As soon as, for example, *Linux* becomes as popular as *Windows*, the viruses will follow suit – probably even more dangerous than the ones we have now. The development of new technology as regards anti-virus protection will help. In addition to this, the now common practice of combining different anti-virus defence methods such as behaviour blocking (sandboxes) will make protection more effective. This is one of the industry's most promising technologies which allows virus detection not by searching for unique signatures but by blocking the virus's activity, which is limited by the application or operating system.

Conclusion

We can point out the breaches viruses can exploit, new applications they can move towards and even useful ways to protect against them. The only thing we are unable to do is to fix so-called 'mind breaches'. Users are responsible for protecting their computers. And nothing, not even the best AV software available today, could be more effective against viruses than the basic rules of 'computer hygiene'.