



Rather than The WildList changing what it lists from month to month to match names established later, including arcane names known only within anti-virus research circles, it would be better for

researchers to consider the name used in The WildList.

It is important for vendors to accept the fact that The WildList is a tool initially conceived to benefit the user. As such, the reason why certain names are used (and will continue to be used) in The WildList is because they are the names that immediately have the most user exposure. For more information on the naming issue and how *WLO* manages things from an anti-virus research organization perspective, see http://www.wildlist.org/Naming_Policy/.

Conclusion

If it were not for reviewers, many of us would not have a clue as to the viability of a product. If it were not for reviewers, many products could possibly go unnoticed. If it were not for reviewers, a large percentage of the population might remain uninformed about how many different products are available. The WildList is a welcome tool for anti-virus software reviewers and certification bodies.

If it were not for users, reviews and certifications simply would not matter. The WildList is an excellent tool for the user. It gives users an accurate picture of which viruses are being found with prevalence. In combination with ItW certifications, it allows them to know how their products do against a *proven* threat.

The WildList is created by those who have a direct interest in keeping the computer virus threat under control (the Participant), and by those who rely on anti-virus software (the corporate reporter) as their first line of defence. If it were not for the Participants and corporate reporters, The WildList simply would not exist. However, because The WildList exists via so many different sources of input, it is an excellent and impartial tool valuable to all.

WLO realizes the positive impact it has in the anti-virus industry. The anti-virus industry also seems to realize and support the many good reasons for the popularity of The WildList, for the generally agreed-upon way The WildList is formed, and for the continuation and further evolution of the *WLO* project.

OPINION

Learning from Experience

Péter Ször
SARC, USA

The other day Eugene Kaspersky told me that a Russian magazine calculated how much money a single virus has the potential to generate for AV vendors around the globe. It is funny to think that an average macro virus could mean much more than our salaries for several months. Seriously, the anti-virus business is nothing like it was 10 years ago when I started to be interested in computer viruses. Or is it?

The Good Old Days

In 1990 I felt I was competing against John McAfee's *Scan* with my own program. *Scan* could catch about 40 viruses at the time and my product could detect and disinfect most of the same ones. A decade has passed and it turns out that I am still a competitor of the legendary software, regardless of the fact that not too many people know what John McAfee is doing nowadays and neither do they remember my first anti-virus effort.

I was lucky to have met Dr Alan Solomon during his active years in anti-virus development. My fear is that this tendency will continue and other heavyweight anti-virus folk will leave computer virus research during the next couple of years. I also think a few smaller vendors will merge into one big company realizing the needs of a bigger market and stronger resources.

It is always easier to predict the future if we take a look at the past. In 1990 there were so few viruses. The number soon exceeded the magical 300 mark and a little later there were thousands of them! A few names pop into my mind: Brain, Jerusalem, Stoned, Yankee_Doodle, Form, Tequila, Michelangelo, DiskKiller and DIR_II. Many of you will remember Ripper and One_Half and lots of others. It was so difficult to deal with the first polymorphic viruses. I remember looking at the MtE-generated decryptors for a week, it was really crazy! I laughed when one of my friends told me that computer viruses would give me a job for life.

I believe the virus of the decade was introduced in 1995. It was WM/Concept.A, the first in-the-wild macro virus to give many companies a new challenge. Before Concept several products had tried to follow the 'detection-without-repair' concept. They soon learned that disinfection is important, especially for corporations.

The Mighty Macro

Macro viruses appeared because the major operating system used on computers slowly changed from DOS to *Windows 95*. Several DOS and boot viruses were compatible

with *Windows 95*, but sooner or later many of them became incompatible with it. However, and most importantly, the system reached a lot of homes on clone PCs and this meant that virus writers had all the resources to create new viruses on it. Developing a binary virus is much more difficult than writing a macro virus in *Word Basic*, *VBA* or *VBS*.

Win95/CIH caused major problems for many big corporations and home users. *CIH* was the first *Windows 95* virus successful enough to cause world-wide infections. *CIH* made history by being the first virus to wipe out the flash-BIOS code, making the hardware unusable.

The author of *WM/CAP.A* (one of the most successful macro viruses ever created) soon got bored with macro viruses and created the first *Win32* virus, *Cabanas*, at the end of 1997. New developments with *Win32* ended up with the *Win32/Ska.A* (*Happy99*) Worm. *Happy99* is virtually everywhere now, one year on from its creation.

The same idea was quickly introduced in a macro virus and many companies learnt about *Melissa* the hard way. Its author has created several in-the-wild 32-bit *Windows* viruses, but the problems he caused with *Melissa* were not comparable. There is a close relationship between macro viruses and 32-bit *Windows* viruses – the main environment of both is *Windows*. As *Windows* gained momentum in the marketplace more viruses have been introduced into it.

It is a long time since I heard about a new in-the-wild DOS virus. Macro viruses and Trojans are causing the problems for most of our customers these days. More and more corporations have to deal with 32-bit *Windows* viruses, too. At the time of writing the number of known 32-bit *Windows* viruses has itself passed the 300 mark. Does that mean that we will have thousands of them out there soon? Absolutely! There will be many new multi-partite viruses with *VBA* and *VBS* as well as 32-bit *Windows* virus infection capabilities. An anti-virus company has even been hit by a *VBS* creation and that shows the problem is already big enough. When *Windows 2000* reaches the market *VBS* viruses will assume real significance.

The Theory of Evolution

I think virus development is set to continue on the Worm front for the foreseeable future. Undoubtedly, virus writers are looking for methods to write real Worms that introduce themselves to remote systems without user intervention. The author of the *BubbleBoy* Worm has already found a successful way to do this. I believe the binary virus creators also will try to adapt this idea in order to create more successful Worms.

Recently, it was revealed that *Microsoft* has not won the 'monopoly' game, after all. There is a definite chance that other operating systems will profit from the impact of this. Personally I have never made any money out of my Unix knowledge (which is very little) and I would not be afraid to see *Windows* disappear from the market.

However, systems such as *Linux* are likely to be employed by more and more corporations. I am not talking about home users. I do not expect them to learn zillions of command-line parameters and walk around with a 1,500-page book entitled 'A Short Course on Linux'! In any case, this particular system will be used increasingly and this means one sure thing for anti-virus people. It is time to consider the *Linux* platform seriously and devote more resources to researching it. You can be sure that more viruses will appear on *Linux* if (and this is a big if) it reaches more homes. Since the executable COFF format is so similar to the Portable Executable format used by 32-bit *Windows* systems, it is reasonable to believe that cross-platform viruses will be developed for *Linux* and *Win32* systems (including *Windows CE*).

Microsoft is dropping the support of Alpha environments with *Windows 2000*. That leaves *Intel* processors the major environment for all operating systems currently significant in homes and corporate environments. *Win64* is knocking on the door and so are *Win64* viruses. Imagine several AV companies still supporting low-end machines. It is funny to deal with the 64 KB limits when virtual memory managers are built into the operating systems. It is going to be no fun decrypting 64-bit viruses (which use 64-bit encryption keys by default) even on those 64-bit machines. A few *Win32* viruses with *MMX* support already indicate the problem.

The evolution of computer viruses is certainly speeding up. Computation power is getting bigger and bigger and this leads to extremely complex polymorphic and metamorphic viruses (viruses that are based not on mutated decryptors, but on modularity).

Caveat User

Bearing all this in mind, what can the 'good guys', the anti-virus people, do in the foreseeable future? We need to work more on automation and spend more time developing generic solutions. This will give us enough time to handle the most difficult viruses most of the time. Virus labs will have to build test environments for testing Worms. One short year ago we could build a test system each time a new Worm appeared, but it is absolutely unacceptable now.

If you are responsible for keeping your corporation's computing environment virus-free, your goal should be to gain extensive knowledge on the security features of your operating systems and applications. There are still large corporations out there with many security holes in their systems leading to virus infections which should not happen in the first place.

It is imperative to keep updating your system's virus detection databases. Heuristics catch a lot of new creations, but you must use the very latest AV databases to get efficient protection. Many companies have 'crossed their fingers' hoping nothing bad happens, only to see thousands of their PCs infected with a virus that could have been caught just by using the latest update for their scanner!