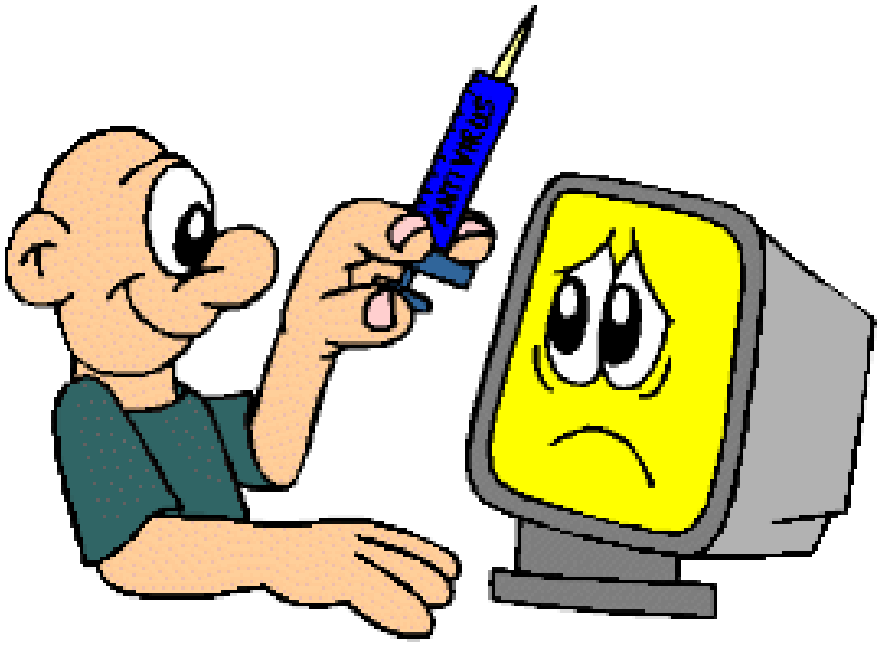
Important criteria for antivirus programs

There are many antivirus programs (CTCV), each with its own strengths and weaknesses. Most CTCs are built based on some fundamental criteria, which is also the basis for helping



There are many antivirus programs (CTCV), each with its own strengths and weaknesses. Most CTCs are built based on a number of foundation criteria, which is also the basis to help you choose antivirus solutions for your system.

Technology

Detection of viruses according to patterns or behavior of malicious programs. A file capable of self-replicating and assigning its copy to another executable file is very suspicious. Most behavioral virus checking methods can check all input content to search for specific code snippets or put content into the 'safe' area (sandbox) to monitor activity and prevent when there is any malicious behavior. Behavioral testing is very effective in detecting new viruses in the 'infected' state of a system before software developers have new virus updates.

The popular 'find and kill' method relies on the database (database) of virus identifiers (virus samples) that developers get from a multitude of different sources to detect viruses. The length of a virus pattern from 8 to 16 bytes will be compared to the files on the machine. Developers must choose samples carefully to avoid errors. According to Symantec, there are nearly 70,000 dangerous scripts, so the virus sample database becomes extremely large. Some developers use 'hashing' to 'capture' the sample, CTCV will 'hash' the file to be checked and compare it to the 'hash' csdl pattern to identify the virus. This is very important, greatly reducing virus

testing.

The scanning mechanism is equally important as the virus sample database, when a new attack type is detected, the old mechanism must be updated. For example, the W2K / Stream virus was discovered in September 2000, its code hid in the special NTFS file structure and at the time no one could detect the virus until the scanning engine New virus is upgraded.

The malicious code program is rapidly increasing, forcing CTC developers to always add new technology and update the virus database continuously, usually several times a year. If your CTCV is 2 years or older, you may be in danger. Some vendors develop a scanning module that can be updated with a virus sample database, but most require installing a new client program, which is usually large, on the user's computer. Please check the carrier's website to understand the mechanism for updating the program and database.

Intelligence: most CTCVs allow smart scanning, meaning that the program will detect and prevent unknown virus patterns (the developer has not updated the virus database). This mode shines inside the code of a program / file to find suspicious behaviors, procedures or tricks. For example, any program that automatically encrypts or attempts to change the core of the system or copy itself is a sign of the virus.

Enabling the 'smart' function may affect the system's performance, although this method may detect unknown risks but may also miss or miss. This is an option in most CTCVs, you can turn it on / off or even adjust the percentage of intelligence.

Efficiency

Accuracy: developers balance between accuracy (analysis) and speed. A 100% accurate scan program can run as slow as a turtle so developers set their default in their products to scan only common file types and let you configure yourself for other file types.

Sometimes a high degree of accurate scanning results in mistakenly receiving problems. Misidentification can be frustrating, but the ability to survive will allow the virus to spread. According to the experience of network administrators, CTCV only needs about 95% accuracy to be able to resist most common malicious codes. There are no CTCs reaching 100% accuracy level. A good virus scanner only needs 97% and sometimes 100%.

Many computer virus researchers believe that the ability to test 100% of current risks is only possible in the experiment. Virus Bulletin magazine (www.virusbtn.com) awards a 100% VB award to CTC which can detect all the mischievous code on the Wild List list (international organization provides free information about viruses, www.wildlist.org).

In fact, many viruses need special tools to destroy (such as Nimda, Klez) and this tool can often be downloaded from the CTC developer's website. Note that you need not only the main version removal tool, but also its variants (Nimda.A is very different from Nimda.E).

Speed: no one wants a slow virus scanner, to compare nearly 70,000 virus samples in database with everything on a user's computer for a few minutes is extremely difficult. Instead, we will scan to which file format strategy has the highest risk level which will be prioritized first.

For example, if you often work with Microsoft Excel (open your files and others), you can configure scanning of Exel (.xls) files first, then other files such as application programs, system files. .

Another problem is the CPU's processing power to both scan and run other applications. Many people believe that virus scanning programs "squeeze" the CPU's ability and slow down the entire system. The most flexible scanning mechanism must allow you to determine the percentage of CPU capacity for its task.

Fix infected files (recovery): When a CTC finds malicious code, you want it best to remove the virus from the system and return it to a healthy state. Some viruses overwrite or delete files permanently, the desire to recover becomes hopeless. If a CTCV estimates that it cannot repair the file completely to return the file as before it was infected, it ignores the repair procedure, which is why most software only isolate the infected file without deleting it automatically. .

Viruses today are in a state of condition, such as writing to the registry, changing the process of booting the system . the virus is removed from the infected file but its harm can still exist!

For example, one of the behaviors of the Nimda virus variant is to create a shared drive for all logical drives on the infected machine. If the visitor to the shared drive has Full Control, it will get worse. This behavior complicates the system administrator's troubleshooting process because Nimda can easily infect other shared drives.

Depth: the need for compression and storage is present everywhere in today's PC environment, it's hard not to find a file compression utility in any PC. Hackers have dozens of compression tools to transform viruses. A CTCV can find the virus in the zip file, but can it detect the culprit in a file that has been compressed multiple times with many different programs? CTCV needs to recognize which files are compressed, to extract, check that the file is still compressed to decide whether to either decompress or scan the file. Especially if the file contains a link to another malicious file, CTCV needs to scan that link file too, this technique is called recursive scanning.

Some CTCV developers claim to be able to scan 20 different compressed file formats, a few say no and almost no product can scan all existing compression formats. Some firms claim their products have recursive scanning capabilities but the results are disappointing.

File with password protection: Another important issue is password protection, a challenge for scanners, most CTCV cannot be retrieved and must be ignored.

In the situation where the file has a digital signature, how does CTC behave? If a registered document or program contains a virus, the antivirus capability will create an invalid new certificate.

For Windows users who use Microsoft Encrypting File System (EFS) to protect their documents, some CTCVs are able to scan where the key codes are stored when users log in to the correct account.

If CTCV does not support NTFS scanning with a boot floppy, you can use Sysinternal's NTFSDOS utility to create an NTFS boot disk. In this way, CTCV can hardly scan compressed files and encrypted files with EFS.

Deployment and Administration

Organization model: If you are administering a typical Windows-like environment, the problem is very simple, but if the complex network infrastructure includes many system platforms (for example, Windows and Linux) then More complex work.

Deployment tools for clients: Nearly all antivirus solutions for businesses have deployment tools for clients (user

machines) remotely. If you're a Windows school, perhaps the Windows application-type tool will get your attention because they run fast, friendly interface, and run smoothly on Windows. For browser-based web applications, administration is similar to web browsing, but you may need web server (IIS, Apache).

Implementation time: The factor depends a lot on the network situation, especially with the situation of converting new anti-virus solutions. There are several organizations that examine and evaluate the timing of implementing each product under standard ('cyclic' and 'clean' cycles and systems to avoid conflicts with other products). However, this is only a reference criterion, not completely determined to choose an antivirus product even if it can shorten some time.

Protection at all times: Virus scanning products should warn a full scan on one machine and real-time protection (realtime). In theory, if a software requires a thorough scan after first installing and running real-time protection, you won't need to scan from scratch. With the network environment, products that support certain remote scanning satisfy administrators.

Update the new model: One problem to consider is the time when the system is in a state of threat to attack when a new virus emerges, which is due to the lack of remedial Windows vulnerabilities. If an antivirus product has a longer recovery time, it increases the risk for your system.

You must regularly update the virus sample database, only consider products that can update the virus pattern search mechanism automatically and daily from the vendor's official website to your server.

The ability to collaborate with another server like mail server: It's hard to have an organization that works without email. Email is a means of communicating with external partners, messages to each other internally and it is also a risk of virus attacks and spyware entering today's largest internal system.

Approximately 80% of the virus spread via email (according to the International Computer Security Association), the ability to integrate with mail server / client becomes an issue of concern for an antivirus product.

Technical assistance

The product website provides as much analysis of virus tricks as possible, especially the 'encyclopedia' to look up the signs of a specific virus. In addition, information about the form of hoaxing virus users so you can be stable before their hoax. Finally and also very important is to allow free download of anti-virus related tools and references.

Epilogue

The complexity of choosing an antivirus product increases with demand, from personal needs to businesses. In addition to information from the developer, you can also refer to independent antivirus testing and evaluation organizations such as Veritest (www.veritest.com) or ICSA Labs (www.icsa. net). ICSA Labs certification is very prestigious in the field of antivirus, most anti-virus products on the market want this 'certification'. Similarly, VB 100% is also a reliable source to select antivirus solutions for the system.

Lighthouse