A DAY IN THE LIFE

The Politics of Anti-Virus

David Ensign
ACS Government Solutions Group, USA

Unfortunately, protecting against computer viruses and other malware is a standard part of any computer support operation today. *Affiliated Computer Services Government Solutions Group* (*ACS GSG*) provides full service computer support to US Federal government agencies across the United States, each with differing missions, operating environments and requirements.

In 1991 most Federal agencies, like many organizations, hoped the computer virus problem would remain isolated. *ACS GSG* received reports of fewer than ten virus encounters in the four years after the first virus appeared in the wild in 1987. Nevertheless, in late 1991, we determined that the threat from viruses was growing and began formulating a protection plan for our customers.

The timing was fortuitous, because the Michelangelo scare arose in February 1992. While exaggerated, it created an atmosphere in which organizations were receptive to anti-virus protection implementation. With draft procedures already available, widespread distribution was accomplished in a matter of weeks. No instances of Michelangelo were found but numerous other infections were, justifying the heightened focus on viruses. As a result, *ACS GSG* devoted a small but dedicated staff to the issue.

Our virus protection philosophy is based on the following tenets. Regardless of how successful the program is, viruses will continue to try to infiltrate from outside sources. Therefore, all plans must be long-term. The key to virus protection is early detection and removal. The only effective early warning system is the use of anti-virus software with active monitoring (on-access scanning). User restrictions (no Internet access, mandatory diskette prescanning) should be avoided, as these usually face resistance, resulting in non-compliance and a negative attitude. Protections should be automatic and invisible to the user (unless a virus is detected).

In the case of an infection, the most important element is an investigation by trained staff – the cornerstone of a successful and proactive virus protection process. This assures that all infections are properly cleared of the virus, there is no continuing threat to internal workstations and media, and the source and all recipients are alerted to potential problems, preventing accidents and hopefully eliminating the source for additional virus incursions.

In order to trigger a support request and ensure an investigation, users should be discouraged from clearing their own systems. Where possible, AV software should be set up to disallow automatic eradications of viruses that reach the desktop. (Unfortunately, few major packages provide options to prevent user-initiated or prompted eradication.)

Data collection associated with virus incidents is essential for tracking containment and gathering critical information to analyse for trends and trouble spots. Where available, automated encounter reporting should be activated.

Recently, we implemented email gateway firewalls with virus scanning. We now have a centralized detector at a single point of entry for email and an automated mechanism for tracking a large majority of incidents, providing a more accurate picture of the virus situation. Due to automated reporting, the firewall can clean and forward the attachment to the user, eliminating any impact on productivity and alleviating the need for an on-site investigation.

With macro viruses the greatest threat today, the email gateway has become the most important weapon in our arsenal (although desktop protection remains the fundamental component of a complete solution), providing a line of defence for everyone, even in organizations that do not have proper or up-to-date anti-virus software at the desktop. In the face of Melissa, it provides a tool for the rapid identification of an outbreak and a viable platform for countermeasures. If you can afford it, implement one; if you cannot, find a way.

Daily Activity

Due to the various reporting mechanisms, we log hundreds of virus encounters every month. Several times a year, we provide one-day orientation courses on viruses and virus response procedures to organizational computer support staff, who take that expertise back to their groups. These trained staff provide the first line of support to users, with *ACS GSG* available to help and to review each incident in order to ensure proper containment (quality control).

Optimally, users who encounter a virus notify their support staff or a central Help Desk. A trained computer support staff member responds to the user and determines the source and propagation of the virus and eradicates it appropriately. Investigation sheets (outlining all applicable questions for each type of virus) are completed and faxed to us for review and logging.

An organization must escalate notification of an incident to *ACS GSG* immediately in four cases: when the virus is new to the organization, the virus is destructive, the virus has infected a shared resource such as a network server, or the virus is network-aware. Our involvement is directed in order to ensure complete containment and prevent loss of data or services, and to analyse any new threat that may require a procedural change.

We also monitor the email gateway scanners, which log every intercepted message. Usually, the infected attachment is cleared and transmitted to the user. The original message lists the source and all recipients, so a complete history of the virus is detailed, simplifying the ‘investigation’. The gateway notifies the sender automatically, alerting them to problems and so eliminating one of the computer support staff’s duties. If the message is outbound (originating from within a site), the appropriate support staff are notified.

Recipient lists are reviewed to see if associated organizational users have received the file, unaware of, or possibly unprotected from, the danger. The gateways have been a boon, eliminating the need to dispatch staff to the many desktop computers that used to be infected each month, drawing precious resources away from other tasks. This alone has recouped any costs for the gateways themselves.

Gateways also have policy checkers that allow them to intercept hoax messages based on the message’s text. We review all of these immediately upon receipt, as they are sometimes legitimate messages that need to be passed on. Hoax messages are not transmitted, greatly reducing the number of calls from users, which used to occur daily, again distracting resources from more important efforts.

Virus reports are monitored constantly for immediate identification of any threats. Summary reports are printed monthly and examined for dangerous trends. A written analysis is provided for corporate computer security and management staff each quarter summarizing the current situation and recommending preventative improvements.

The Internet provides an easily accessible informational avenue to staff and users. We use it to distribute AV software and updates. Most anti-virus software business licences allow for home use and employees can install and maintain the software at home much more efficiently through Internet access. We maintain Web sites at customer locations for education, hoax information, and analyses.

A Recipe For Virus Protection

1) Complete protection means an anti-virus program on each and every desktop computer. With today’s propagation volume, any chink in the armour is susceptible to virus invasion. The desktop is the single focal point for the major virus types and must be the place to centralize protection.

2) Active monitoring (on-access scanning) is the only viable desktop implementation. Periodic scanning, even daily, provides a large window of opportunity for viruses to spread in an interconnected environment. Melissa, arguably the most dangerous virus to date, attacks upon infection, so periodic scanning will never provide protection.

3) Procedures and mechanisms to roll out the latest AV updates must be in place. Melissa spread worldwide in three days. You must be able to update signatures as soon as they are released. Monthly (or even weekly) updates are no longer sufficient. For timeliness and resource efficiency, network distribution is the only viable avenue in any large company. Do not rely on users to pull the updates; push them out whenever possible.

4) With macro viruses now to the fore, email is the primary propagation vehicle. While beneficial to virus writers, it also provides centralized points of control that can be used for protection. An email gateway can provide significant protections that will soon recoup any costs.

5) With viruses spreading through so many avenues, a multi-tiered protection architecture is beneficial, and protections should be placed wherever possible (e.g. servers, post offices, gateways, firewalls). We have found that no single package is perfect all the time – implement different programs at different points, both horizontally and vertically, especially in a large enterprise. This increases the possibility that a virus slipping through a gateway, for instance, will be caught at the post office or desktop.

6) Install or activate any reporting mechanism you can, especially automated ones. With viruses, there is no substitute for the awareness that statistics can provide. Many virus problems occur only because they are not seen, and many disasters could easily be avoided with a minimal amount of information.

7) Make sure you have two-way lines of communication with your user community. With the recent publicity about viruses, users are more attuned than ever to the situation, and they can be excellent sources on new threats. Encouraging users to send all alarmist messages to a clearing house will forestall any widespread panic and allow you to update your email policy checker to stop them. Users must be partners in any anti-virus campaign. Use every means to educate them and keep them informed, and be sure to have an emergency broadcast mechanism for use in a crisis.

8) Think about the big picture. Worrying only about your small community will not help in the long run; you will continue to be bombarded by viruses from outside, often from the same source over and again. Notifying originators can alert them to problems they can correct, reducing them as potential sources in the future. Every office and user that implements proper protections decreases the number of avenues through which viruses can propagate.

All this has a cost, but the price of not doing it could be astronomical. Incidents occur daily that justify a high-control approach. Our recipe minimizes virus encounters, and we have the expertise to respond to situations with skill and speed. The virus problem is growing, and new techniques in propagation and payload create a world where dedicated staff are no longer a luxury – they are a necessity.