Editorial Thoughtscapes
Words Impact Business Success
www.et-writer.com

B2C Technology Story

Web Summary:

The Computer Virus Threat: What You Should Know?

by Leon A. Enriquez

Reading Time:
8 minutes

Reader Benefit:
♦ Understanding today's computer virus threat;
♦ Addressing viruses that corrupt and destroy our valuable information systems;
♦ Some ideas on how to deal with the virus threat in a proactive way.

The virus threat is often "more serious" than we tend to give these malicious code the serious attention we give to other security violations. The real cause for concern are the viruses that accompany our messaging systems that most modern day businesses have come to rely on, i.e., our electronic mails.

A typical virus intrusion is through e-mail attachments. Another common occurrence is from material downloaded from the Web. The concern here is that we've become so accustomed to using such information systems so routinely – that we somehow forget that the Internet represents "an easy means of infection from sources with a hostile agenda."

The Computer Virus Threat: What You Should Know?

by Leon A. Enriquez

The virus threat is often "more serious" than we tend to give these malicious code the serious attention we give to other security violations.

After all, virus attack in present times have gone beyond the obvious, e.g., viruses hidden in programs available on floppy disks or CDs.

The real cause for concern are the viruses that accompany our messaging systems that most modern day businesses have come to rely on, i.e., our electronic mails. A typical virus intrusion is through e-mail attachments. Another common occurrence is from material downloaded from the Web.

The concern here is that we've become so accustomed to using such information systems so routinely – that we somehow forget that the Internet represents an easy means of infection from sources with a hostile agenda.

Just remember this: virus represent a real threat to system security. And the real cost of a virus outbreak – in business disruption and lost business opportunities as well as the time wasted to resolve the problems created by malicious code – can often escalate to tens of thousands of dollars. Like fraud, this is often a rather embarrassing situation and so people tend to say nothing about it.

Consider the harsh realities of a virus attack – from help desk personnel to IT managers, every resource involved with the fallout of a virus outbreak – will cost you money!

This cost is directly affected if a company's business is solely dependent on your desktop systems which do not run updated anti-virus software. Costs escalate further if your organisation also has e-mail, a gateway, and other server-based applications and solutions.

Undetected Outbreaks

The idea that a virus may propagate unintentionally is no longer valid. Note that the virus may propagate in isolation in a company as well as propagating through cross-infection, from one company to another.

Such malicious viruses can cause data loss, data corruption, and even alter data characteristics. These incidences may severely impact your business activities and transactions if a substantial volume of valuable data and information resides in your computing systems.

The difference between a computer virus and other programs is straightforward: a virus is designed to self-replicate, i.e., make copies of itself.

A virus usually self-replicates without the knowledge of the user. A virus often contains a "payload", i.e., actions that the virus carries out separately from just self-replication.

Many people believe the worst a virus can do is to format your hard disk. In fact, this type of payload is now considered harmless – for those of us who back up our important data.

The more destructive viruses are those which subtly corrupt data. For example, consider the effects of a virus that randomly changes numbers in spreadsheet applications by plus or minus 10% at a stockbroker.

Other nasty viruses post company confidential documents in your own name to some of the alt.sex Internet newsgroups – an act which can ruin your reputation, and the company's confidentiality.

Consider the commonplace situation where the virus infection goes unnoticed and therefore, undetected. If the virus has no obvious payload, a computer user who does not have anti-virus software installed on his or her computer, may not even be aware that the computer has been infected.

A computer may be infected by virus in several different ways. *(See Box Story 1: First-Time Virus Infections)* A computer that has an "active copy of a virus" on its machine is considered infected.

The manner in which a virus becomes active depends on the type of malicious activity that particular virus has been designed to achieve. For example, macro viruses become active if the user simply opens, closes or saves an infected document. Each time an application is run, there is a potential infection situation.

Once the virus is active on the computer, it can copy itself to "infect" other files or disks as these are accessed by the user. Different types of viruses infect computers, and each in specific ways. The most widespread virus types are macro, boot and parasitic viruses.

To overcome these virus hazards, a company needs to employ a multi-layered approach to virus defence. An effective strategy should include integrated protection – from the Internet gateway to groupware, file servers, and desktops.

There is no doubt that the data virus is a big threat to the security of programs and data. Fortunately, users can adopt some measures to reduce this danger. *(See Box Story 2: Anti-Virus Housekeeping.)*

Obviously, the daily challenges facing the corporate information security experts put a premium on prevention rather than cure. Through such real-life scenarios, a big picture of what's important in selecting anti-virus protection software emerges.

Businesses today are increasingly dependent on computing environments – connected via the Internet – that are both highly distributed and connected globally. The obvious benefits of migrating to a multi-platform, networked architecture are substantial.

In addition to streamlining operations and reducing costs, enterprises can rapidly expand business capabilities through deployment of newly evolving platforms such as mobile devices, Web services, and other online applications.

Clearly, a centralised end-to-end management of the "virus outbreak lifecycle" is needed to deal with this modern-day security threat. Not surprisingly, transitioning security operations to one with an enterprise protection strategy is a significant first step. This means building a kind of robust, scalable, and standards-based foundation. This will then go beyond anti-virus protection to support a comprehensive enterprise security architecture.

Although e-mail has revolutionised the way companies communicate both internally and externally, e-mail content security is no longer just a matter of virus protection.

Today, companies need an effective solution that provides protection from virus attacks and malicious code, while offering protection from internal employee violations of company policy and sabotage.

The increased reliance on the Internet has changed the methods used to spread viruses. With the widespread adoption of e-mail, a new headache has arisen for corporate IT administrators. A new generation of mixed-threat e-mail-borne viruses have emerged to threaten the corporate messaging system.

Box Story 1:

First-Time Virus Infections

Examples of first-time virus infection are:

1. Diskettes used by an outsider who may access the computer; or diskettes used on an infected PC at home;
2. E-mail attachments;
3. Programs acquired from a developer infected by virus;
4. Programs downloaded from the Internet;
5. Programs developed by a dissatisfied employee or former employee;
6. Diskettes used on an infected computer and later distributed.

Box Story 2:

Anti-Virus Housekeeping

To reduce the risk and danger which viruses represent, you can resort to the following anti-virus housekeeping.

- ***Security Policy***

Implement a general good security policy:

1. Tell the users about security hazards, including those that are virus-related.
2. Wherever possible, isolate your critical systems from potential infection sources such as the network and Internet.
3. Software programs installed on computers must be for authorised use. Restrict and monitor the use and installing of new programs on computers.
4. Make certain that sufficient control mechanisms are in place. This includes the administration of the system as well as virus control.
5. Make sure that virus infections are discovered, and reported promptly. This means that you can install a virus control program which is updated by new virus definition files, as and when these are updated and published.
6. Inform users about the different warnings which a virus control program will use to inform the users about potential virus presence.
7. Take corrective action and relevant steps to restrict the propagation of a virus when it is detected. For example, check all disks which have been used on the infected computer, check the documents and check the servers.
8. Make sure that everyone knows how to react if his or her computer is infected. All users must know the person this virus incident or problem must be reported to.
9. A backup crisis team is a good resource to have and can be helpful.
10. Make certain that you can re-install critical programs, and data from a backup which is not infected by virus.
11. If such a backup does not exist, learn how to remove viruses.
12. Be aware of new infections from a virus which was supposedly removed.

- ***Prevention***

1. The best way for users to protect themselves against viruses is to apply the following anti-virus measures: when a virus attack has occurred, you can then retrieve safe copies of your files and software.
2. Inform all users that the risk of infection grows exponentially when people exchange floppy disks, download Web material or open e-mail attachments without caution.

3. Have anti-virus software installed and updated regularly to detect, report disinfect viruses; remember, if you do not regularly update your anti-virus software with the latest anti-virus signatures, you may be exposed to virus attacks from new malicious code strains.

Box Story 3:

Watch the Three Virus Entry Points

There are three main entry points in your network computing environment where it makes sense to deploy anti-virus software, namely, on the Internet gateway; on the servers; and on the desktop.

Internet gateway
The Internet gateway is the point that connects your internal company network to the public-domain Internet. It is a good place to install anti-virus software which will check incoming and outgoing e-mail attachments.

The main advantage of using anti-virus software on the gateway is that incoming infected attachments sent to multiple e-mail addresses will generate a single virus alert should the infected e-mail escape detection and goes through to the desktop.

Servers
Using anti-virus software on servers to scan centrally held files has several advantages over trying to scan the servers from a workstation.
#1: Network traffic is minimised since the scanning processes runs locally on the server.
#2: Any virus stealth mechanisms are not effective since the virus is never "active" on the server.

Desktop
Virus scanning on the desktop is probably the most important part of the three-point scanning strategy. If the virus penetrates the Internet gateway scanner by arriving in an encrypted e-mail, it must be detected at the desktop before it can cause damage by infecting your system.

It difficult to keep desktop anti-virus software up-to-date as this is one of the hardest tasks faced by the IT administrator. This is especially the case for mobile PC systems such as laptops, which are not permanently connected.

About the Author

Leon A. Enriquez is managing editor and business manager of Editorial Thoughtscapes – a professional writing firm. Leon can be reached at leonenriquez@et-writer.com.

<ENDS>