VIRUS, Very Important Resource Under Siege

Tony Reid, Customer Support

Summary

This white paper provides home users with an introduction to viruses, their prevention and related security issues. It is written with novice computer users in mind.

April 2004

Document ID: WP_20040513_01

Lewis Media
Opening a World of Possibilities

Contents

VIRUS, Very Important Resource Under Siege

The world's first virus was discovered back in 1981, its aim was to infect the Apple I computer. Although the theory for self-replicating programs was talked about many years beforehand – in fact as far back as 1949!

Almost everyone who owns a computer has at one time been infected by a virus or at the very least knows someone who has been infected by a virus.

What is a virus?

A Virus is a computer program that's purpose is to infect your computer with the primary intention of replicating itself. Occasionally they have a payload of malicious code intended to damage your computer or files, but ultimately its chief purpose is to self-replicate.

Typical examples of these malicious attacks would be anything from erasing data from your hard drive, altering files, or reconfiguring programs (such as Microsoft Office or your internet browser). Other behaviour can be as simple as displaying messages or sending out hundreds of emails(Spam advertising) from the user's computer - usually without the user being aware of this. Of course when this happens, you will notice a complete slowdown on your internet connection and degradation in your computer's response times.

More recently, viruses have been produced with the aim of creating backdoors (open ports) in a victim's computer, allowing hackers to remotely perform tasks from an infected computer rather than their own. In some cases viruses have infected thousands (usually hundreds of thousands) of computers with the aim of a timed parallel attack on large corporate websites. This form of attack is known as a distributed denial of service attack – or more commonly known as DDOS. A diagram of such an attack can be seen in Figure 1.

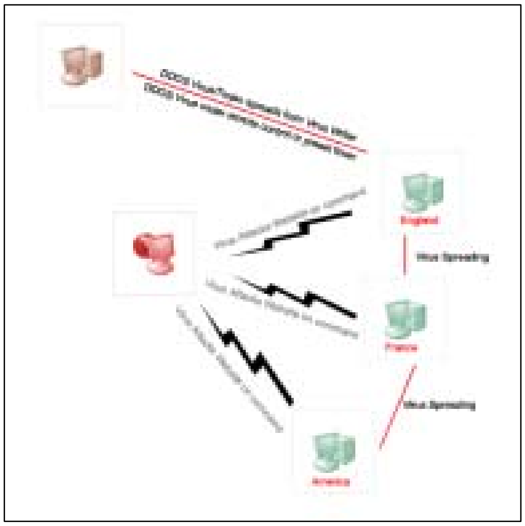

Figure 1: Distributed Denial of Service Attack

In simple terms, DDOS is when thousands of infected computers request pages from your website at the same time. This has the effect of overloading the web server and in most cases causes it to either crash, or run to a halt.

Imagine over 250,000 infected computers attacking your website or computer once every second.

How do viruses infect computers?

One of the basic requirements of a virus is self-replication. In general – each time a virus runs, it copies itself and attempts to infect another program. Or indeed if terminated manually by the user, a typical virus would reinstall itself.

Viruses jump around computer systems, via CD-ROM's, Floppy disks, Email, USB memory sticks, etc. Any form of digital travel that they can make use of will be used. More advanced viruses interlope around computer networks via networking protocols and exploit holes in computer operating systems like Windows 2000/XP – this type of virus is called a worm because of its worm like nature.

What types of viruses are there?

Common types of Virus are Macro, Boot Sector and File Infector

Macro Virus

Microsoft's feature intense packages such as Office, Visio and Project contain a flexible programming language, which provides companies and individuals the capability of tailoring the software, and also add custom features. This programming 'macro' language is called VBA – or Visual Basic for Applications. It is a very flexible and powerful scripting system that virus authors have learnt to manipulate for there own usage.

Thanks to VBA, word documents and the like now have the capability to carry a virus.

File Infector

The aim of a file infector virus is to attach itself either parasitically or via association with an executable program/file. Each time the host program is run, the file infector spreads itself.

A File infector spreads by passing infected files around, either by floppy disk, CD or email etc.

Boot Sector Virus

A boot sector virus infects the first sector of a disk. This is a special area that the computer that the computer needs to access when you turn it on. Its also an area of the disk that doesn't 'usually' get wiped when you format the drive – and so reinstalling your computers operating system will not necessarily clear the virus. Like File infector viruses, boot sector viruses tend to be spread by the users sharing disks or via pirated software rather than by any advanced programming technique.

How can I tell if a virus has infected my computer?

There are thousands of symptoms/signs that your computer could be suffering – too many to list here. The best way to determine that your computer is clean is to install anti-virus software.

Obtaining anti-virus software for free is possible and some commercial companies offer their software free for home users and only charge for commercial users.

AVG Antivirus is available free for home usage via www.grisoft.com
FPROT Antivirus is available free for most operating systems via www.f-prot.com

There are many more anti-virus products out there, and a quick search on Google will identify many commercial anti-virus vendors.

How can I prevent being infected again?

The best way to prevent re-infection is to regularly update your anti-virus software. It used to be that a monthly update or bi-weekly update was sufficient. However, most technologists recommend updating at least weekly, and many recommend daily. Most anti-virus software has build in scheduling tools to do these updates automatically.

Commonsense also plays a big part in virus prevention. Be suspicious about emails that you were not expecting – If you get one that you don't like the look of; update your anti-virus software before opening it.

Virus Scan any media that you have not had full control of! A 30 second scan, could save you hours of reinstallation.

Conclusion

We have discussed the types of computer viruses and the basics of how they move around.

Hopefully you will now understand why keeping your anti-virus software up to date is a must – especially as new viruses are being developed every day.

It is also a good idea to sign up to a vendor's anti-virus security alert email service – as they are free and often your first alert that a new virus has been discovered.

Happy virus hunting

About Lewis Media

Founded in 2001, Lewis Media is a Kitchener/Waterloo-based business that was born under the philosophy that high-tech doesn't need to be high-priced. With the programming background of the original four founders, Lewis Media is able to offer web-development services to small and growing businesses previously only available to larger corporations. Focus on delivering custom tailored solutions to their customers, Lewis Media stays true to their goal of having every customer say, “We trust Lewis Media.” More information on Lewis Media and Lewis Media’s services are available at www.lewismedia.com.

Lewis Media Professional Services

Lewis Media offers a full spectrum of unique professional web development services available in-person, on-site or remotely.

Lewis Media WebAdmin$^{\text{TM}}$

As a web site owner WebAdmin$^{\text{TM}}$ gives you the power to update key information on your web site from anywhere at any time. Changes are made in real-time to your web site, saving you from the delays and costs associated with making those changes through your webmaster. As a webmaster WebAdmin$^{\text{TM}}$ facilitates and simplifies the process of making web site updates, meaning your company’s site can be maintained more easily and efficiently.

Simple Machines Forum$^{\text{TM}}$

Through a unique partnership with Simple Machines, we are able to offer the latest version of Simple Machines Forum$^{\text{TM}}$ to our customers free of charge. Make your site sticky by using the repeat visits generated by a discussion forum. Develop a customized look to your forum or sign up for our “evergreen” service to keep your forum automatically updated and protected from hacks and cracks.

Additional Services

- High-tech web hosting for our development clients featuring several advanced libraries and add-ons.
- Monthly site analysis to track traffic, server loads, errors and search engine queries.
- OpenWeb$^{\text{TM}}$ managed web site system for professionals with exacting standards and limited time.
- InfoFeed$^{\text{TM}}$ technology to automatically update your site with time-critical information.

For more complete information, or for a demonstration of any of Lewis Media’s services visit www.lewismedia.com or contact a Lewis Media representative by phone or mail.

Lewis Media
421 King Street N
Waterloo, ON N2J 4T3
+1 (519) 747-4949
www.lewismedia.com

Lewis Media
Opening a World of Possibilities