Lake County Contractors Association

Professional Practice Report

OCTOBER, 2001

Virus Protection - Do You Know Where That Data Has Been?

By William W Zeigler, CPA Zeigler Associates, Ltd

There was a time that you might have wanted to see a virus just for the intrigue of the matter, just to see one because you never had. And like a tornado, once you saw and experienced the pain and expense of one you'd rather never again. But unlike a tornado or lightning, these days it seems very likely after a first encounter you will continue to see more than you care to.

With the proliferation of Internet connected systems, and the increase in general sophistication and skill level of users in general and the talented elite in particular, nastier bugs are arising more frequently with more exotic names and more powerful damage potential. Virus writers' motivation [and unfortunately their identity] is not always clear. A few bugs are actually unintentional. Some seek true malicious damage to unseen targets perhaps for the glory of hitting the news. With recent tragic events now in our history, we may think of more aggressive and dangerous intentions intentionally crossing international borders that we have yet to see. In any event, protection now needs to be addressed if you wish to avoid reformatting your hard disk [or 100 others in your e-mail list] or worse, replacing your system due to actual physical damage.

Here's a few examples with which the writer has direct experience:

SirCam [Sep 30, 2001] – I have received numerous e-mails with almost the same text: "Hi! How are you? I send you this file in order to have your advice. See you later. Thanks." Attached to the e-mail is an XLS or DOC attachment with a PIF extension which is an old style Windows executable program file. This is another one of those that collects e-mail addresses to send itself out potentially to known recipients to the sender. The Virus Encyclopedia also states: Aside from e-mail overloading, it may delete files and/or fill up hard disk space by adding text entries over and over again to a SirCam recycle bin file. Defense? Simply don't download this file.

Nimda [Sep 18, 2001] - You notice this little bugger because on your Windows desktop, in almost every folder on your disk and program group in your startup menu you see unsent e-mail messages. Delete them and they magically reappear a few seconds later – hundreds and perhaps thousands of them. Try to run some programs and you encounter memory error messages. As of updates released the last week of September, virus protection software will permanently eradicate the code from the system but programs are already damaged and need to be reinstalled – including Windows. This one can also damage memory on the motherboard requiring its replacement.

MTX [Aug 2000] – This one ends up disabling your ability to connect to the Internet although that's not its intent, which is to collect entries in the address book and send itself out to those addresses. This is a tough and prolific little bugger to try to avoid reformatting the hard disk or using the most recent virus protection data. Reinstalling Windows even to a fresh directory and reinstalling all applications still saw the bug transfer from hidden places in even unused directories to the new one.

Tristate [Feb 99] – This is an Office Visual Basic Code modifier, quickly replicates through all Office data files in all Office applications. It usually disables any code already in the file, removal requires cleaning all files on all computers at the same time even on a network or it just reappears even in a file cleaned seconds earlier.

One protection website has identified 36 new viruses discovered in just the last 30 days. In almost all cases, they released a fix the same day, in all the remaining cases except one [which took 5 days to fix] a fix was available the next day. And just to stir your noodle more, there are viruses that are designed to look malicious and

Professional Practice Report is a publication of LCCA's Professional Service Committee. LCCA is not responsible for the content of this article which only expresses the opinions of the author. For more information, contact LCCA at 1312 Washington St., Waukegan, IL 60085 Phone: (847) 623-2345 Fax: (847) 623-2349. Past reports are available on the LCCA Web Page at www.lcca-il.org.

dangerous but actually do nothing except trigger detection in protection software. There they are just playing with you!

Virus protection procedure and software is becoming more of an issue as time passes right now. In this cat and mouse game, virus software also increases in effectiveness and power. Honestly, some years past I was more reluctant to recommend installing virus protection and enabling all features. Virus protection programs work by intercepting processor commands, disk reads, e-mail reads, file downloads – and checking them before completing those commands. The earlier, less efficient programs on slower systems were a serious detriment to performance and actually created system errors on occasion. Today it is different. Performance is less of a concern on today's fast systems. The software is more efficient even as viruses have become more complex.

One way to protect your system is to never come in contact with a bug. Some users address this by never connecting to the Internet or using a floppy disk. While this is effective, it is like avoiding car accidents by never driving – the utility of being connected is tremendous and the real trick is to be connected to gain those benefits and avoid infection. Assuming you remain connected, recent bugs are using the e-mail system for transport – you are a willing participant in transporting the code to your system yourself. Usually, these e-mails contain some attachment that you copy to your local hard disk and then open or run thinking it is something else – the damage is usually done instantly. The conventional wisdom used to be to not download any e-mail from someone you know. Some recent viruses are using your address book and sending an e-mail to a recipient who knows you, so this advice is little protection now. And worst of all in this e-mail world, a limited few viruses transmit by simply reading an e-mail even if there is no attachment.

What do you do about this group of threats? Virus protection software now monitors your e-mail and your downloaded attachments. The danger is detected and damage prevented as you perform your normal activity. Further, as the brain of your system performs commands, the protection software monitors the effect and intention of the command in case the brain encounters a psychotic break.

The cat and mouse game now has evolved on the protection side to a process to update the program with an expanding list of known viruses and ever-increasing commands to clean the virus from infected files. The most important point to take from this article is that you should obtain these updates frequently - usually by downloading from a website and running a file that adds the new protection to your installed program. All systems I have cleaned had virus protection installed, but it was never updated – in one case the protection code was two years old.

On a related topic, in recent years as their cost has declined and availability increased, super-fast and always-open Internet connections are fast becoming prevalent. These provide a constantly visible if not accessible door allowing a bad-intention connection for access, retrieval and deposit of destructive code or information. In a subsequent article we can look at Firewalls, the tools that protect unauthorized access into your systems and files usually through these constantly open connections.

In conclusion, virus protection software has clearly become a necessary evil. Perhaps as it has become more necessary and thus in wider use by a more interested and responsive customer base, its effectiveness has also improved at an increasing rate. Thus, previous concerns on its use have diminished at worst to manageable and tolerable levels. So go for it – install it and use it.

Professional Practice Report is a publication of LCCA's Professional Service Committee. LCCA is not responsible for the content of this article which only expresses the opinions of the author. For more information, contact LCCA at 1312 Washington St., Waukegan, IL 60085 Phone: (847) 623-2345 Fax: (847) 623-2349. Past reports are available on the LCCA Web Page at www.lcca-il.org.