Stay Safe Online Campaign's
AntiVirus Presentation

by Chengi Jimmy Kuo
McAfee Fellow
Network Associates, Inc.

Introduction

Welcome to the Stay Safe Online Campaign. This is the AntiVirus (AV) technical presentation.

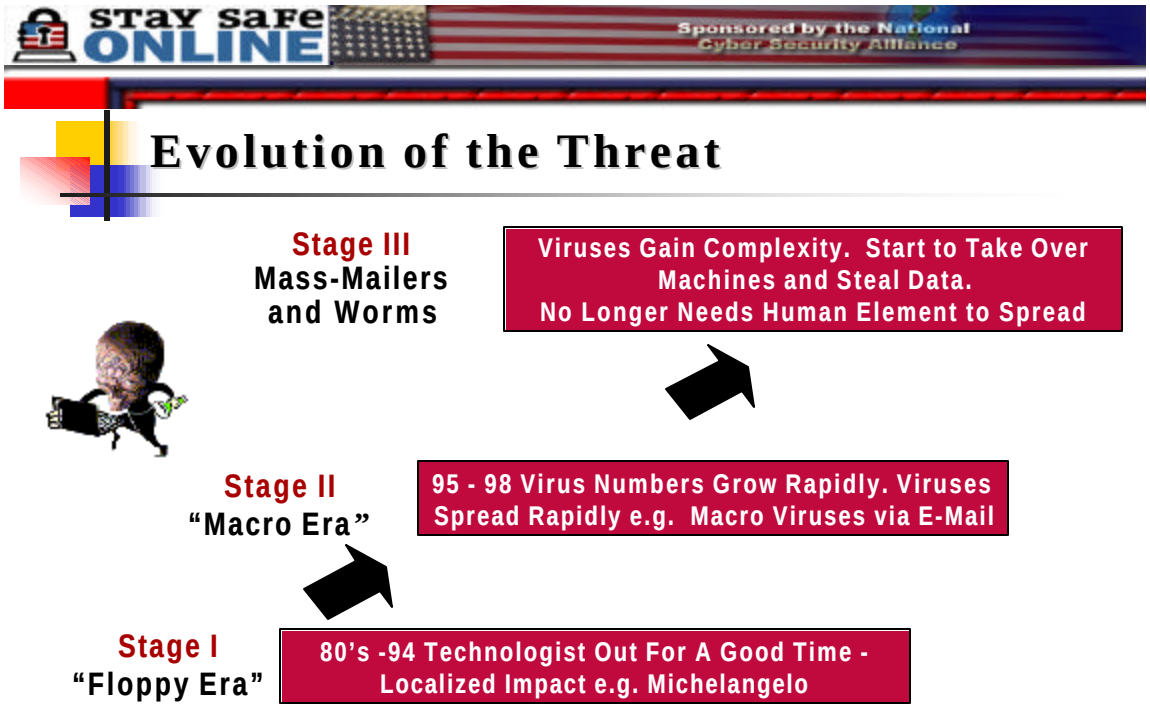
What is a virus?

The common belief is that anything bad happening on a computer is caused by a virus. Not so. Viruses are programs that spread. A traditional virus spreads by attaching from program to program. Worms, a term recently in vogue, generally spread from machine to machine. But a worm is a type of virus.

Trojans do things you did not expect and is not documented. And you believe the author did it on purpose. If the author did not do it on purpose, it would be called a "bug." And if you liked what it did, you would call it a "feature."

An exploit involves the deliberate misuse of something the author did not intend. Automated worms that spread without human interaction will usually involve an exploit. Personal firewalls can be used to hide exploitable software from being vulnerable to the Internet. AV software can block some of the known exploits. But to really fix an exploit, one has to update to the latest version of the deficient software.

Evolution of the threat



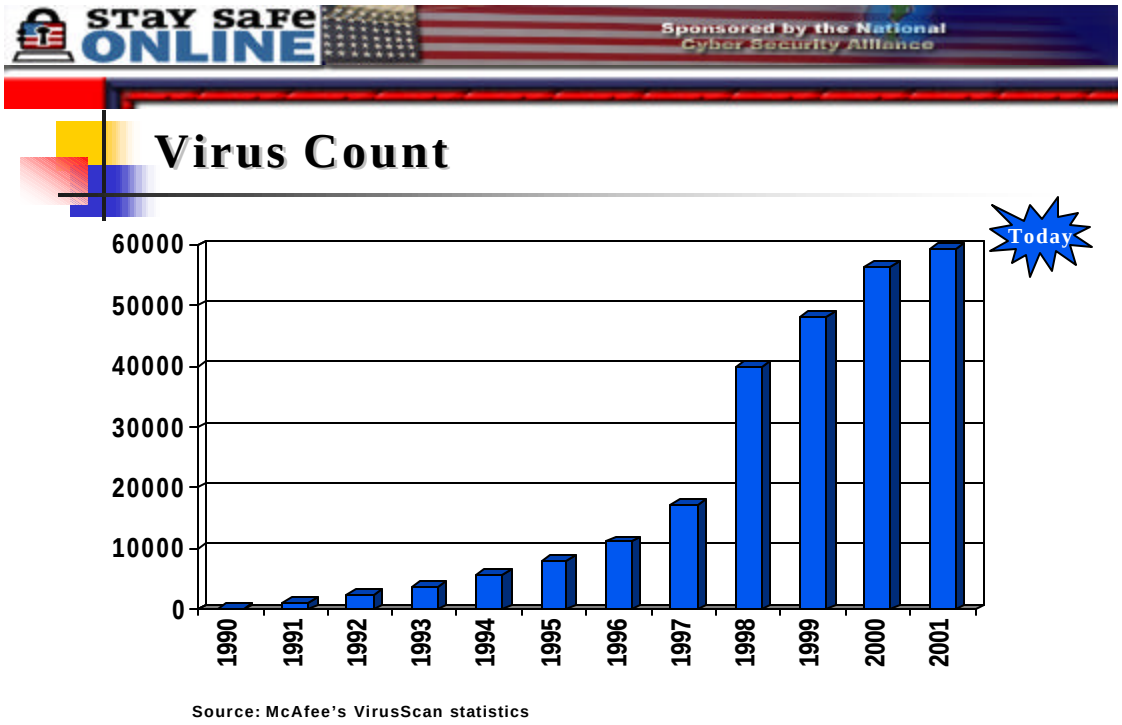
The floppy era was characterized by its use of floppy disks as its replication medium. That made the travel and spread of viruses quite slow. Sneakernet was the word used to characterize such distributions. Viruses attacked files in the DOS operating system. And bootable floppies were responsible for the spread of boot viruses. Viruses named Jerusalem, Stoned, and Michelangelo dominated.

The macro virus period followed. It involved primarily Word documents and Excel spreadsheets becoming infiltrated by viruses. Previous to this, we only considered executable programs to be infectable. Now document files became suspect. People no longer used diskettes so boot viruses died. The department server was the main virus distribution medium. So usually, when someone in the department got infected, the whole department was infected. Melissa, a macro virus mass-mailer, bridged the gap to the present period.

Which brings us to today, where most everyone has email on the Internet. And many people have high-speed access directly from home. And some even run businesses with web sites thus leaving their home machine on the Internet at all hours.

This offers a rich environment enabling worms and mass-mailing viruses to reach many, many people on the Internet. If you could remember the television commercial, "She tells two friends, and she tells two friends, and so on, and so on, and so on." All of this connectivity has enabled viruses to overwhelm the Internet and reach worldwide distribution in a matter of hours or minutes. Viruses are combining traditional viral techniques with vulnerability exploits. This creates the situation where no humans are needed to spread viruses any more, although people are still very useful in this regard. Once seeded, the viruses can now spread themselves.

Virus Count



The graph shows the progression through time as the number of viruses continues to grow year after year. There is exponential growth until 1998. After that, it becomes more linear. This is caused by a number of factors.

First, there is what I'll call, the Law of Big Numbers. That is, exponential growth can only go for so long. Then the numbers get too big to maintain that pace.

Second, people count viruses. Particularly, people who have to study and fix the problems are doing the counting. This works out pretty well because it makes us think, "What can we do so we'll have less work? And less stress?" The result is a concentration on detecting viruses without need for updates. If AV is able to detect and clean new virus variants, users will be less affected. And fewer affected users result in less stress for antivirus researchers. (Yea!) You see. The work of an antivirus researcher is very much like that of a fireman. When there's a fire, it's an obvious emergency. Every minute counts. And it's very stressful. But all in all, we would rather there was never a fire. We would rather have stopped the blaze before it became widespread.

Because of this work, more viruses are now detected as generic members of existing families. When that happens, users don't have to send the samples to the antivirus researcher's lab. If it never shows up in our lab, it doesn't have to be studied and possibly distinguished from existing variants. And thus, the number of known variants is not increased. (And less work for us!)

The last reason though is unfortunate. We now see many more worms and more complex viruses. A single person could have been written CodeRed. But Nimda was definitely written by a group. So, instead of potentially five people each turning out single-minded viruses, we got one walloping, sophisticated virus. Virus writers around the globe have formed virus writing clubs, and now cooperate to create fewer but more rapidly spreading and damaging viruses.

We ended 2001 just shy of sixty thousand viruses. This compares to one thousand in 1991, and ten thousand in 1996.

Some popular viruses

I have just mentioned the CodeRed and Nimda viruses. These two have been in the news recently and carry specific characteristics of interest. In the next sections, I will talk about those two and a couple other viruses that have some special effect, especially as they affect our future.

LoveLetter

The LoveLetter virus is noted as the most costly virus incident ever. It was the first widely distributed virus making use of the .VBS extension. Much of the cost attributed to this virus is due to the virus' effect of overwriting all files bearing the extensions .vbs, .vbe, .js, .jse, .css, .wsh, .sct, .hta, .jpg, .jpeg, .mp2, and .mp3. All such files were replaced by copied of the virus, and the filename changed to add a .vbs extension. (We call this the payload.) And the most cost occurred to those who did not keep proper backups of their data. The most affected were small businesses, unable to maintain the proper backups, and heavily dependent on their website operations. So, let me highlight the importance of maintaining backups.

The virus initially arrived as an email with the following characteristics:

Subject: **ILOVEYOU**
Message: **kindly check the attached LOVELETTER coming from me.**

File attachment: **LOVE-LETTER-FOR-YOU.TXT.vbs**

As a first of its kind in using the .vbs extension, system administrators at the office were unprepared for it. This allowed the virus to become so very widespread. The combination of a widespread scenario with damage to files that were not backed up accounts for the exorbitant damage figure of over eight billion dollars worldwide.

Now, also note the double extension. That was another first. Depending on how one's system is set up, the file may appear to the user without the true extension of .vbs, resulting in a user's belief that the file was a harmless text file.

Mail flood caused by the mass-mailing aspect of LoveLetter is mostly a thing of the past. Those susceptible to mass mailing have had their friends and neighbors yell at them sufficiently to rid themselves of the virus. However, LoveLetter persists today as one of over 100 known variants. In a file-sharing environment, what you may believe to be an MPEG or JPEG file might instead be a LoveLetter infected file with the .vbs extension hidden from view. If you are not properly protected, you not only become a new vector for the virus, but at some point, your music and picture files will be overwritten.

Lastly, the alleged perpetrator of this virus was quickly apprehended in the Philippines. But unfortunately, laws needed to prosecute the offense were not in place and had to be developed from this event. And the perpetrator was set free.

CodeRed

[slide 8] CodeRed is a perfect example of a worm. I use the adjective "perfect" because there is absolutely no file component to this virus. (Recall that worms are viruses too.) Therefore, the virus must be detected in transit or in the memory of an infected machine. Traditional desktop antivirus products looking for files on a machine will have nothing to find.

CodeRed took advantage of an existing exploit in IIS (Internet Information Server) 4 and 5. Thus the solution to this problem involves fetching the patch available from Microsoft at:

http://www.microsoft.com/technet/security/bulletin/MS01-044.asp

or any subsequent cumulative patch. If you are not sure of your system's status, then try the patch. It will tell you if you are not a candidate for the patch.

The CodeRed (and Nimda) virus travels using the HTTP protocol (port 80). This is the same channel used for Internet web queries. So, if you run a web server, you need to secure that machine against such attacks. And if you do not run a web server, you should block all port 80 access to your machine. Doing so will inhibit Nimda and CodeRed from attacking your machine, and inhibit future worms that might choose the same route.

The historical lineage of the different CodeRed variants starts with CodeRed.A. .A didn't work well. .B was injected into the Internet on July 19th at about 1300. .B's introduction killed .A. CodeRed.C, or CodeRedII, was released August 4th about 1200 GMT. And it subsequently killed .B! But it was coded to stop spreading after October 1, 2001 after leaving a backdoor on infected systems. Finally, .D is a minor copycat variant of .C that coexisted for a while and died similarly on October 1. Without .C and .D to kill it, there are sporadic sightings of .B. But fortunately, the number of vulnerable machines has diminished greatly.

The damage attributed to CodeRed is much less than that of LoveLetter. Part of this is because some of the machines were subsequently taken over by Nimda. And thus, the cleanup cost goes under the Nimda column.

Nimda

Nimda is what some call a virus cocktail, or a blended threat. It makes use of at least 5 different attack modes, including making use of backdoors left by previous viruses.

Coming soon upon the heels of those other viruses, it meant there was not much time allowed for its development. Thus we conclude a team of people, not just a solitary virus coder, likely developed it.

Who could that have been? We don't know. A bunch of teenagers? We doubt it. Elements of a foreign government? Maybe.

But what it shows is that if we don't protect ourselves, our own machines could be universally commandeered and used against us in a matter of hours or minutes.

The Nimda virus made use of the following attack methods:

- Mass-mails README.EXE.
- Gathers email addresses from one's mailbox and cached .HTM[L] files
- Email will execute immediately on receipt on vulnerable systems.
- Infects web pages.
- Viewing infected pages results in automatic download and execution on vulnerable desktops.
- Infects files by appending to .EXEs.
- Converts C and D drives to open shares.
- Uses a number of Unicode exploits.
- Uses backdoor left by CodeRed.C/D to infect.
- Uses backdoor left by Sadmind and others to infect.

An estimated quarter million to a half million machines were overcome by the virus. And many of those machines were well-known www sites, or mail servers for medium to large companies. In total, over fifty thousand important Internet sites were infected. The good news is, they're mostly all fixed now. And certainly all the important ones in those big to medium companies. But many thousands of home users still have not fixed their machines.

And, wouldn't you like to know how we know all this?

When an infected machine tries to infect others, it sends commands to its neighbors (on the Internet), and some long-distance friends as well. Those are the previously mentioned exploit commands and the backdoor commands used to commandeer trojanized machines.

Anyone on the Internet can see those indiscriminately directed commands. It's like stationing the town crier in front of your house yelling, "The back door of my house is open! Come get whatever you want!" This is actually the most damaging aspect of this virus!

You can see it today if you have a personal firewall. Look at all the HTTP (port 80) attempts that it blocks. Each one is issuing an invitation for a bad guy to come and scour the machine for any juicy information. You certainly don't want bad guys looking through your machine!

To close many of the exploits used by Nimda, please download the following patch, labeled:

29Mar01 Incorrect MIME Header Can Cause IE to Execute E-mail Attachment
http://www.microsoft.com/technet/security/bulletin/MS01-020.asp

It's Just Text

Before I depart from telling you about the dangers of the new viruses that have come along, there's just one more… Unfortunately, a new virus infection method has rendered inaccurate the last "safe email" rule we had.

Previously, we taught users that text only email messages were completely safe from viruses. Unfortunately, this is no longer strictly true. In August of 2001, a new virus type was shown in concept. And in December, it was used again. The first was a virus named Loding. In December, Coolsite.

These viruses come to you as a message with no attachment, no code, but does contain a URL. Accompanying the URL would be an enticing message to click on the URL. Certain mail programs will highlight the URL in a different color, and allow you to go directly to the website should you click on that URL.

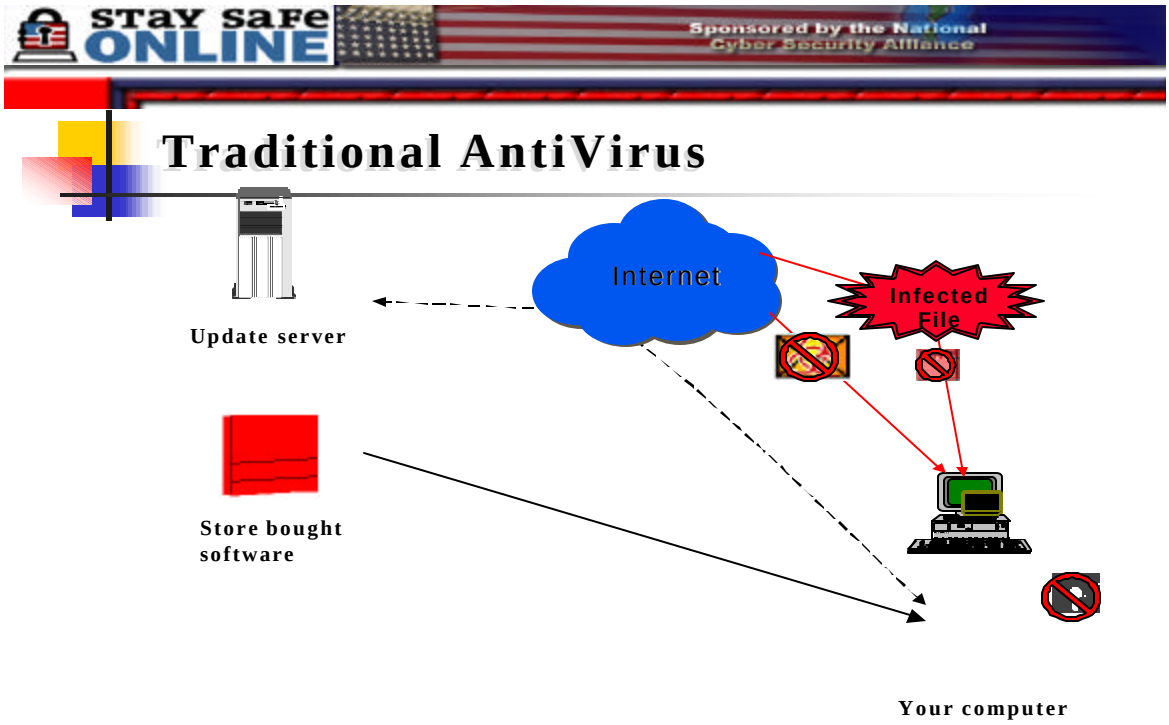
The HTML code at the website unfortunately is programmed with an exploit that then reads your address book and forwards this virus to all your contacts. (This is what the viruses have done. But they are not limited to that.) So, if a message from your friend just doesn't seem right, be wary of it. And ask your friend about it before proceeding.

As the code takes advantage of an exploit in Internet Explorer, I recommend that you download and execute the following patch:

http://www.microsoft.com/technet/security/bulletin/MS00-075.asp

In the meantime, the antivirus researchers will use our contacts to close down such sites as quickly as we can. Viruses of this nature need to coordinate through their chosen website. And if we can close it down immediately, it will render the virus impotent. And that's what was done with each of the first two cases.

Traditional Antivirus



I need to spend some time now to describe the use of antivirus products.

Traditionally, people would buy an antivirus program in a store. After installing, the first thing to do would be to update the program and associated data files. There's no telling when the box version was created and shipped from the factory, and many thousands of new viruses have probably been discovered since then. Updating one's AV is usually but a single click, and the software will take care of itself. If your preferred AV doesn't work that way, please check the supplied instructions. But an antivirus product is considered only as good as the last time it was updated. Once updated, your machine will be protected against malicious programs and emails from the Internet, and also viruses entering the system through diskettes.

Other AntiVirus Methodologies

There are other ways of acquiring antivirus protection. It is possible also to purchase antivirus online, rather than through a traditional store. The same processes and protection levels are achieved, except the online distributor assumes immediately that you have an Internet connection. (Well, of course!) Thus notifications and updates are likely to be more automated.

Many antivirus companies also provide online scanning capability, usually free of charge. You can submit your machine to be scanned online. Or you can submit suspicious files and get an online or an email reply message. The difference between this offering and the aforementioned packages is that free online scanning only acts when you request a checkup. It offers no protection during any other time you might be using your computer. So, the user must keep up with security issues himself. So, the service is usually used to ascertain the cause of recent strange behavior on the system.

Also available on the Internet are email screening services. This is where your email provider offers to check your email before it is transferred to your email reader. This may be less costly than a full antivirus package, does not use any of your system resources, and you leave maintenance issues to the email

administrators. But similar to the online scanner provision, your machine remains unprotected against any other threats. However, if combined with a properly configured personal firewall, and up-to-date patched software to keep out exploits, this may be a sufficient choice.

What you can do

So, what does all this boil down to?

The purpose of this National Cyber Security Campaign is to inform and educate computer users, especially home and small business users who do not have the assistance of hired computer security experts. We urge you to read, understand, and put into effect the Top Ten Tips. Awareness of the issues conquers half the problem. Then you can create your own personalized solution. Or if you choose not to be protected, you'll know when to be more careful.

Number One on the Top Ten Tips list is the suggestion, "Use AntiVirus Software." It substitutes for the hired computer expert. It keeps a constant eye on what's coming into your computer.

But you have to update often. Update weekly or according to the schedule provided by your antivirus provider. Also, any time there is an issued virus alert. If you don't update, there won't be protection against new viruses. And as you saw, hundreds are discovered each month, at minimum.

Lastly, don't open messages from strangers. And don't open strange attachments from anyone!

Compare what you've just read to the security of your front door. Don't let strangers in. Don't pick up suspicious packages.

Most of all, stay alert! The easiest way to stay secure is simply to keep one's eyes open and notice if there's anything out of the ordinary.

Keep yourself safe from viruses and Internet attacks and everyone around you will benefit.

Thank you

Thank you for taking the time to participate and in doing your part to secure the Internet for the safe and enjoyable use of everyone. -- National Cyber Security Alliance

About the author

Jimmy Kuo is a research fellow with McAfee, the antivirus division of Network Associates, Inc. He is a 1982 Bachelor of Science graduate of the California Institute of Technology in Pasadena, CA. In addition to McAfee, he has served in research and development for Symantec, IBM, and Locus Computing Corp. (now Computer Associates). He is the founder of McAfee's AVERT (AntiVirus Emergency Response Team) and co-author of one of the first research papers on computer viruses on IBM PCs.