

Hacker Prevention Techniques

By Aaron Turpen

Hacker Prevention Techniques

Aaron Turpen

aaron@aaronzwebworkz.com

Aaronz WebWorkz <http://www.AaronzWebWorkz.com>

Permission is given to reprint this article in any medium provided the author's bylines remain intact.

=====

Hacker Prevention Techniques

by Aaron Turpen of Aaronz WebWorkz

I remember when the term "hacker" referred to a computer geek who could transform a mundane electronic device, with a few modifications, into something completely different from what the manufacturer and designer had envisioned for it. In some cases, these were cool improvements and more than one of these hackers made a fortune selling the rights to them. In other cases, the transformation just made you wonder if the guy's horn-rimmed glasses were a little too tight.

Nowadays, the term "hacker" is used to denote a nefarious individual who, for one reason or another, causes havoc or harm to computer systems. The old "hacker ethic" - sort of a code of honor, like the Samurai Bushido code for computer geeks - is apparently no more. The new "hackers" of the old school are now "open source" participants ("coder" is a popular term for them). A "hacker" is now someone who breaks into systems, proliferates viruses, sneaks in via a trojan horse, or otherwise causes problems with other's computing.

The Spread of Attack

Currently, the variations of the Klez virus are reported to be the most prolific online spread of malicious code. Luckily, all it really does is find your Outlook address book and perpetuate itself with your contact list. The news media is always quick to pick up on the latest "hacker attack" or "computer virus infiltration" and make sure it's a top story for the day.

With all of these perceived and realized attacks, how do you, Mr. and Mrs. Internet User, keep yourself and your data safe?

Most of us are aware of the need for "firewalls," "anti-virus software," and such. Hopefully, most of us are using these tools to protect ourselves. Beyond that, however, there is more you need to know. First, we'll cover what the attacks are.

Know Thy Enemy

There are five major forms of attack commonly used against personal computers and networks. Some are more common in attacking one while others are for the other.

DDoS (Distributed Denial of Service) Attack – usually aimed at networks, this type of attack focuses on open ports and connections in the network or system to flood them with requests and “pings” in order to overwhelm it. This is akin to the Mongolian Hordes descending suddenly upon a city before the citizens had time to react and defend themselves. Usually the attacks are made by third-party systems that are probably unaware that they are part of a network of attackers – compromised systems or systems with little or no security are usually the unwitting accomplices of the hacker.

A DDoS Attack can seriously undermine a network by causing one or more systems and their resources to shut down or crash, removing them from use. An example of this type of attack would be the recent attempt to close down the majority of the American Internet backbone in October.

The good news is that the majority of the major systems, as witnessed last October, while temporarily hampered by these attacks, recover completely and easily from them. Most networks are now self-monitored by software that “roves” the network, watching for outages or unusual occurrences. Most server software now includes “flags” that watch for unusual activity and suddenly pop up to let the network monitor know that something may be amiss.

Trojan Horse – this is the electronic version of the downfall of Troy. Basically, software disguised as something else (sometimes something useful) makes it way to your system by your own hand – you wanted the software, right? This software usually contains a “back door,” a “trigger,” or something similar. A “back door” allows someone to enter your system while you're using the software and do what they wish. The more common “trigger” method waits for a certain trigger (a date, a time, a series of events, etc.) and then sets itself off like a bomb. The results can be any number of things from system shut down to the sudden launch of an attack using your computer and its network or Internet connection. It's not uncommon for a trojan horse to be spread around as the part of a DDoS attack – triggered to all go off at the same time.

A perhaps less malicious, but no less worrisome, version of this type of software would be the SpyWare available on the Internet. This is software that performs a neat function – like Gator filling commonly-used form fields for you – while also collecting information about you to send to advertisers and marketing companies.

These are by far the hardest things to find. Until someone notices what they are, they won't be reported to be cared for by any anti-virus software companies or “spyware” lists. By downloading shareware and freeware, you are taking the risk of installing one of these onto your system. For myself, this is a risk that I have to take as there is way too much great software out there for me to limit myself to only what I can find on the shelf at the store. It pays to read the terms and conditions carefully and to note where you are getting the software from. If it's from a source you don't know well (this includes eBooks and the like!), you may want to reconsider whether you really NEED to download that software or whether it's available from a more reliable source.

Virus – this term is fairly commonly used by people, both online and off. Everyone has heard of a computer virus at one time or another. They are the most common and usually the most sensational of the five major attacks. A computer virus functions in the same way a biological virus does. It's primary concern is usually reproduction. If you think of each computer connected to the Internet as a cell in your body and the network connections (email, data, etc.) as blood vessels transporting lifeblood (information) from one computer to the next; it's easy to see how a computer virus (usually spread via email) can reproduce itself (make copies) and spread from one system to another quickly. Most viruses focus on this point above all others – many times doing nothing more than spreading themselves. Others spread themselves and then destroy or attempt an attack on the host system (the system it is currently on).

A good example of the virus, as already mentioned, is the current Klez epidemic spreading from

computer to computer around the 'Net.

The two best defenses against this virus are, luckily, generally included with most new computers: anti-virus software and a network firewall. If you keep your virus definitions up-to-date, scan your system regularly for viruses, and make sure that a functional firewall is in place, you will avoid most virus attacks. I, myself, get about a dozen flags from my anti-virus software every day as viruses are sent to me by various people online.

Websites – Most people are unaware that certain Web technologies have “holes” that can be exploited by less than stellar individuals who build malicious websites. These sites, using known security holes in technologies like ActiveX, Java, JavaScript, and others, can trigger your web browser to start doing things to your system. For instance, a well-known hole in an older version of ActiveX allowed the entire contents of any one folder or directory on your hard drive to be automatically uploaded to a web directory or emailed to a receiver. Another hole in early versions of JavaScript allowed the writer of the script to cause Outlook (in Internet Explorer) to silently send an email to anyone, effectively giving your email address away to the website owner for a SPAM list.

If you are using the latest versions of your browser or limit your use of Internet technologies, you are in little danger from these attacks. Usually, once the security hole is found, patches and fixes are quickly available before anyone can take advantage of the holes to any large extent. If you are running a newer version of your browser of choice and have the latest patches and updates for the various plugins you may be using, you should be relatively safe from this type of attack.

Worm – finally we come to the last of the big five. The worm is much like a virus, but usually serves a different purpose. A worm is kind of like a tapeworm in your belly. It consumes and consumes resources until finally it's too large for you to host or you die from its thievery. On some levels, a worm is a combination of a DDoS and a virus attack. Worms usually reproduce as often as possible (growing) to spread as widely as they can. However, a worm's primary function is to suck resources. In most cases, the worm is built for a certain type of system (a PC running Windows 98, a Linux server running Apache, an Apple computer running OS X, etc.) and is benign to all others. Once it finds its intended target, however, it begins sucking resources – usually quietly – until the system finally becomes overloaded and ceases to function.

The Klez virus has been deemed a “worm” by some, though instances of it taking over resources are not common. Worms are most commonly aimed at larger systems (mainframes, corporate networks, etc.) and some are built to “consume” data and filter it back out to someone who shouldn't have it (corporate spies, for instance).

For the average Internet user, a worm is of little consequence and is usually covered by the same software that protects you from viruses. It must be said, however, that worms are sometimes undetected for quite some time as, like a trojan horse, it usually has to do something before it is noticed.

Gearing Up For Battle

Now that you know what you're up against, you should understand what it is that you'll need to combat the beasts.

Most of the items you need are probably included on your computer already – many are free to download as well!

The recommendations I'm making are my personal preference. There are other versions of these same types of software (some of which I'll mention) and no one can really tell you which is better for you. Most of the software mentioned is available for both PC and Mac.

Anti-Virus Software

I prefer Norton Anti-Virus (I use it as a part of Norton Systemworks) for virus protection. I find it easy to use, easy to buy, and well-made. The updates are frequent and do not take long to download (they average 100-300 kilobytes per download, with releases about once a week).

Another anti-virus software with a solid reputation is McAfee. Most new computers come with one or the other pre-installed. You can buy either from Amazon.com or at your local software store.

Firewalls

A firewall is the term used for software (or hardware) that functions like a firewall in building construction: it completely blocks the path of a fire – delaying or halting its progress. Firewalls on a computer block network traffic coming to and leaving a system, giving permission to transmit and receive only to those pieces of software authorized by the user.

My favorite firewall software is ZoneAlarm. Available for free for individual users and at a nominal fee for professionals and businesses, this simple-to-use software takes care of everything most users will need. It alerts you when unauthorized software is attempting to send or receive (thereby letting you authorize it or find the culprit) and the Zone Alarm site has a large database of known software so that if you aren't sure what's trying to access, you can click on the warning box and a web page will open with an explanation of what that software is (if it's in their database).

I'm not aware of any comparable software firewalls available. There are a lot of hardware options, though, especially if you connect via broadband. Most cable and DSL modems are now equipped with built-in firewalls for protection.

You The User

By far the best tool for defense against attack of any kind is you and what you know. If you know what you're up against and ways of combating it, you are less likely to be a victim. The uninformed user is more likely to stumble into or unwittingly be the progenitor of an attack. If you are in the know, keep your software updated, regularly update your virus definitions, read informed articles such as this one (*wink*), and watch for sudden changes in your computer's activity – you'll be better able to defend against attack.

We will probably never be able to keep all attackers and attacks from causing harm. But at least we can minimize their effects or reach. As J. Edgar Hoover once said, “for every thousand honest men, there's one hoodlum trying to steal from them.”

=====

Aaron Turpen is the proprietor of Aaronz WebWorkz, a web services company providing web design, development, traffic, and more. www.AaronzWebWorkz.com

Get-Articles.com : 1000's of reprintable business and internet marketing-related articles.

[Submit your article for reprint.](#)