A Web of Lies

Today's online threats and what to do about them

Nobody wants to return to the days when the Internet was science fiction and people exchanged data using floppy diskettes, but that ancient era of computing was much better than the one we're within today in one major regard: **malware**. Short for **malicious software**, these are the viruses, worms, keyloggers, and other programs designed to do everything from stealing your personal information to simply breaking your computer.

It's not as if malware didn't exist before the Internet Age, but back then, it was much more contained. Malware generally had to be put on a floppy disk that had to be inserted into a computer, or someone had to physically sit at your computer to put it there. Once installed, the damage it could do was also fairly contained because home networks were unknown, corporate networks weren't very large, and malicious software coders tended to target individual machines.

The Internet changed everything. Its popularity and ubiquity eliminated the need for malicious software programmers to have physical access to the machines they prey upon while simultaneously granting them access to millions of potential targets. According to a study conducted by Panda Labs, which scanned nearly 2.5 million computers for malware in the fourth quarter of 2012, 42.97% of those PCs were infected with at least one type of malware.

Malicious software programmers have to do three main things to install their handiwork on your computer. First, they must decide what type of program they want to install, then they must package it, and finally, they must deliver it. In this article, we tell you what types of threats to watch out for when heading online and what you can do to stave them off.

Types of Malware

With rare exceptions, every malware program has a purpose. Determining that purpose is vital if you want to figure out the best way to keep that type of malware off of your computer or wipe out an existing infection.

Spyware and adware. These work just like their names suggest. Spyware keeps tabs on one or more aspects of your computer usage. Some spyware captures passwords you enter, and other types of spyware monitor your browsing habits to profile you. The bottom line is that spyware tries to capture personal and private information and provide it to someone who normally wouldn't have access to it.

Adware is software that displays ads on your computer that normally wouldn't appear. Sometimes it works in conjunction with spyware to tailor the ads to your personal habits based on information collected by the spyware.

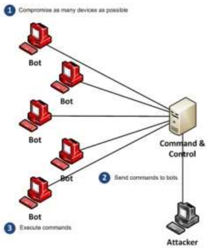
Removing spyware and adware requires dedicated antispyware/antiadware programs. The antivirus software that most people are familiar with won't work unless it also has an antispyware/antiadware component.

Keyloggers and screen scrapers. Wouldn't it be awful if someone could see everything you type on your computer? That's what keyloggers do. They store everything you type and pass it along to someone else.

Screen scrapers are similar but in many ways worse. These take screen shots of your Desktop at regular (or programmed) intervals, letting someone else see exactly what is displayed on your computer screen throughout the day. Many keyloggers and screen scrapers are installed by someone who has access to your computer and wants to spy on you, but an increasing number of keyloggers are showing up that are installed remotely and used to harvest passwords.

Keyloggers installed by people with access to your computer are sometimes physical devices that are inserted into a USB slot or between the keyboard cord and the computer's keyboard port. More often, they are software detectable by good antispyware software, but if they were installed by someone you know, they may have disabled your antispyware or put the keylogger in the antispyware's whitelist. This is a list of software the antispyware program automatically ignores, so check your software's whitelist every so often to make sure nothing fishy is in there.

Botnets. One of the biggest uses for malware these days is infecting as many computers as possible with a program that is either set to activate on each infected machine at the same time or that can be remotely triggered by the malware programmer. These bots can then be used to do anything from obfuscating illegal communications to sending floods of simultaneous requests to a particular Web site and causing it to crash (called a DoS, or Denial-of-Service, attack).



Bot software is extremely difficult to detect because it is designed to hide itself and doesn't do much of anything until called upon. Many bots can be removed using antivirus and antispyware software, but getting rid of some of them requires using specialized tools specifically designed to take care of a particular type of bot. Many of these tools are made available by antivirus and antispyware companies, and Microsoft also releases several tools and fixes that are installed when you update Windows.

Destructive Malware

A decreasing amount of malware exists solely to do as much damage to the target computer as possible, but it's still out there. These purely chaotic programs may delete the entire hard drive, prevent the computer from booting, or simply cause programs or Windows to crash. Sometimes this is by design, and other times, it is because a poorly coded piece of malware goes out of control. Either way, the results can be devastating. Regular use of antivirus and antispyware software generally takes care of destructive malware.

Some attacks change your browser's default search engine, so if you see weird search results, it's time to run an anti-malware scan.

In the past, a decent antivirus product was enough to keep the baddies from infecting a PC, but threats are becoming increasingly sophisticated. These days, multiple utilities are required to prevent or eradicate infections because malware is packaged in so many different forms. We'll talk about delivery methods in the next section, but the basics are to never trust programs linked in emails, be extremely careful about the download sites you use, and scan all downloads with your antivirus and antispyware software before installing them.

Viruses. Computer viruses got their name because they behave in many ways similar to biological viruses. They infect a system as soon as they come into contact with it, replicate themselves, and then try to infect emails or other user-transmitted files so they can continue infecting other systems. Most viruses have been studied and cataloged. They can be stopped and removed by up-to-date antivirus software.

Worms. Worms are like viruses in that they replicate themselves, but unlike true viruses that require a user to perform some action (such as sending an email) before they can spread, worms can propagate to other machines without any outside help at all. This ability to spread automatically makes worms much more dangerous than viruses, and it is important to keep your antivirus software as up-to-date as possible so it is inoculated against worms.

Trojan horses. These programs are extremely devious because they appear to be programs that offer value but contain a hidden payload that installs malware on your computer. For example, you may download a game that appears to work normally, but in the background, it is infesting your PC with unwanted software. Trojan infections are extremely difficult to prevent because the user installs the software manually, which typically bypasses defenses such as antivirus and antispyware software. You need antivirus and antispyware to remove existing infections, and sometimes special removal tools are also necessary.

Rootkits. Of all the packaging methods discussed in this article, rootkits are the nastiest by far. They are cleverly programmed to install themselves in undetectable places and then access the fundamental core—or root—of the operating system. Once it has control of that, it can do anything, including disabling software that could potentially detect it, granting remote control access to all aspects of the computer to a malicious programmer, and even establishing redundancies so that if it is somehow removed or disabled, it will automatically reinstall itself.

The best-programmed rootkits are immune to antivirus software and can only be removed using specialized rootkit removers or by completely reformatting the hard drive and reinstalling Windows from scratch.

Delivering Malware

Sometimes, just visiting a malware-infested site can change your browser's home page to something that benefits the malware programmer.

Now that you know what malware programmers want from you and a little about the tools they use to extract that information, it’s time to see how they use the Internet to deliver their payload and learn what you can do to refuse shipment.

Infected downloads. The most common malware delivery method is to infect files that users download—inadvertently or otherwise—and manually install. One increasing trend is malware programmers creating authentic-looking Web sites that offer free anti-malware software that actually is a Trojan horse designed to install malware on your computer. According to the Anti-Phishing Working Group’s 2008 Phishing Activity Trends Report, these rogue anti-malware programs ballooned in number from 2,850 in July 2008 to 9,287 by December 2008. Your best defense is to scan all downloads with antivirus and anti-malware software and never download anything linked in an email or that comes from a site you don’t trust.

Piggyback software. A common malware tactic is to hide in plain sight by infecting a program that is then downloaded by the target. When the program is installed, the malware is installed with it.

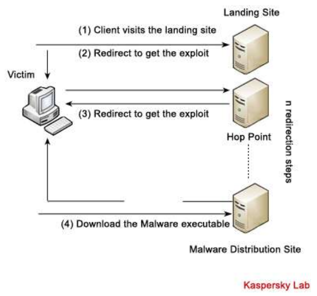
Spam and phishing. The best way to trick users into installing the most effective malware, such as rootkits and Trojans, is through email. Spam, or unsolicited email, is sent out that contains a link to what seems like a legitimate program but is actually malware in disguise.

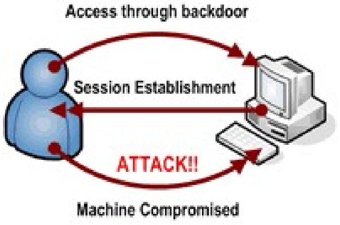
Phishing takes this a step further by including a link to a Web site that looks legitimate but is, in fact, operated by crooks. They harvest information such as usernames, passwords, and credit card numbers that victims unwittingly type into the site, or they post legitimate-looking software downloads that contain malware. Phishing used to be limited mainly to email, but now it is also used in blog comments, forum posts, and practically every other place on the Web where users can join discussions or post comments.

The best ways to avoid these scams are to use a spam filter on your email account, use a browser that has antiphishing technology and can tell you whether a site you’re visiting is legitimate, and to never click a link in your emails or on blogs.

Browser hijacks. Clicking a malicious pop-up window or downloading tainted software can lead to browser hijacking, where your browser is reprogrammed to display ads and point to sites that make money for the malware programmer. The hijack may change your default home page, prevent you from downloading antivirus or antispyware programs, or display tons of pop-up advertisements, among other things. You can avoid this by using a pop-up blocker (built into most modern browsers), not clicking pop-ups, and not installing software unless it comes from a source you trust and has been scanned by antivirus and antispyware programs.

Drive-by downloads. Sometimes, the mere act of visiting a site lets malware programmers take advantage of security holes in your browser and install malware without you clicking or manually installing anything. Keeping your browser as up-to-date as possible and using browsers other than Internet Explorer (a popular target for malware writers) can help prevent this problem.


Landing Site
(1) Client visits the landing site
(2) Redirect to get the exploit
Victim
(3) Redirect to get the exploit
Hop Point
n redirection steps
(4) Download the Malware executable
Malware Distribution Site
Kaspersky Lab



Backdoors. Sometimes, malware (usually in the form of a Trojan or rootkit) creates a virtual backdoor to your computer that lets malicious programmers circumvent the usual Windows login process and gain complete access to your computer. In many cases, backdoors are used to surreptitiously install malware directly onto your computer without any intervention necessary on your behalf. Backdoors are notoriously difficult to get rid of because they can remain open and undetected even if the malware that created them is removed; therefore, reformatting the hard drive and installing Windows from scratch is often the only option.

Protect Yourself

Malware programmers tend to attack the vulnerabilities in Internet Explorer because it has the most market share of any browser, and therefore, they can reach more victims that way. Using an alternative browser, such as Mozilla Firefox (www.mozilla.com/firefox) or Google Chrome (www.google.com/chrome), is a good way to cut down on potential avenues of attack. No matter what browser you use, it is imperative to keep it up-to-date, as vulnerabilities are tracked down and fixed constantly.

Install one antivirus package and one or more antispyware utilities and keep them, along with Windows, up-to-date. A firewall, which inspects all incoming and outgoing Internet traffic to see if you authorized it, also is an important tool in your anti-malware arsenal.

Beyond that, good browsing habits are your first line of defense. Think twice before downloading anything from the Internet or clicking links when you don't know where they lead. If you follow these general rules, you'll make life much harder for the bad guys.

MALWARE RED FLAGS

Malicious software programmers are crafty, and if they do their job right, you won't even know they've been there. Fortunately, very few of them do their job right, and many are so blatant that it isn't difficult to know that something fishy is going on if you know some of the telltale symptoms of a malware infestation.

If any of the following things happen on your computer, be sure to update your antivirus and antimalware software and use both to run complete scans.

- **Home page hijack**. If your browser's home page suddenly changes, and you haven't authorized the change while installing software or manually made the change using your browser's settings, it usually means a malware programmer has hijacked it. They set it to point to a site that loads more malware on your machine or that gives a little bit of money to the malware programmer each time their page loads in your Web browser. If this happens, run a complete antivirus and anti-malware scan, reset the home page to your liking, and see if it sticks. (You can typically find the home page setting in your browser's Options menu.)

- **Unidentified browser toolbars and bookmarks**. Sometimes when you install software, it asks if you want to install a browser toolbar, as well (the Google and Yahoo! toolbars are two common examples), but sometimes malware programmers deliver their software via an unauthorized toolbar installation. Similarly, malware programmers sometimes use browser exploits or illegitimate software to load unauthorized bookmarks or Favorites into your browser in the hope that you'll click them and load a site that installs additional malware or pays the programmer money. Hiding or deleting these toolbars rarely works because the malware that put them there in the first place likely still lurks on the computer.
- **Strange search results**. Your browser has a default search provider that is used when you type entries into the Search box. If this changes from what you're used to seeing to something else (especially if that something else isn't a major search site such as Google or Yahoo!), there's a good chance you're the victim of browser hijacking.
- **Emails asking for account information**. If your bank or any other institution sends an email asking for your account password or other information it should already have on file, delete the email. Don't click any links, call any numbers, or otherwise respond because it's likely a phishing attack. Use the phone book or the number printed on the back of your credit or debit card or bank statement to contact the institution directly and see if the request is legitimate.
- **Nonstop pop-ups**. Pop-ups that appear even when you have a pop-up blocker enabled or that show up even when your Web browser isn't open indicate that malware or adware is installed on the computer, so run complete antivirus and antispyware scans.
- **Antivirus and antispyware stops working**. If your antivirus and antispyware software suddenly becomes inaccessible, or you can no longer visit the manufacturers' Web sites or download updates, it's not a good sign. Something awful is installed on your computer, and you'll likely need to seek professional help to get rid of it if you don't want to wipe the entire hard drive and start over.

adapted from Smart Computing by Tracy Baker