Volcano.net User Guide - Malware Help

Contents

Volcano.net User Guide - Malware Help

Malware

What is Malware?

Malicious software or malware is a category of software that is designed to compromise computers, steal data, and create profit for illegitimate products and criminals. Malware includes viruses, trojans, worms, spyware, and bots and can cause any number of unwanted things to happen to you and your computer. From just annoying popups that won't go away, to your files being held ransom for payment or your personal information being stolen.

Malware also can make a computer unusable, slowing down normal processes or displaying constant popups.

How does Malware get on a Computer?

Malware gets on computers a few different ways, but there are steps you can take, and actions you can avoid that will help lessen the chances of your computer being infected with malware.

Malware Installation Methods

- Social Engineering
- Email – Attachments and Links
- Social Networking Sites
- File Sharing Programs and Networks
- Pirated Software
- Fake Security Popups and Warnings
- Free Games, Screensavers and Themes
- USB Drives

Social Engineering

The people who design and distribute malware rely on a person's trust or lack of knowledge to trick and deceive. This is called social engineering and is the primary technique used to get individuals to install malware on their computer**. A social engineering attack is accomplished by claiming to be a known contact, or a familiar or otherwise legitimate organization or company, thereby gaining an amount of initial trust and then using that trust to gain confidential information.**

An example of social engineering would be an email being received claiming to be a relative of yours, with a file attached. You may feel that because the sender is someone you know, that you can trust this email. But after opening the infected attachment, malware is installed and a hacker then has access to your files. The attacker has used a familiar contact to gain your trust, tricking you into installing their malware.

Social engineering is also used outside of cyberspace. You may have heard someone asking you questions about personal or financial information and once you start asking questions back, they hang up. Or in worse cases, the caller is able to convince a person to give up their personal or company information. The same types of things can happen online.

Email

For many people, receiving an attachment in an email from a friend might be the latest picture of their kids, and that would seem to be a safe thing to open. But the criminals know that's how we think and take advantage of our innate trust of those we know.

Today, a primary method of distributing malware is email. Whether it is an email attachment or a link to an infected server, email is an easy and cheap way for malware to be sent to pretty much anyone who has an email address. If an attachment containing malware is opened, or you go to a site that has been designed to infect computers with malware, these dangerous programs will be installed on a computer. They will then execute their code and do whatever they were programmed to do, and will make your life a little harder for a while.

Social Networking Sites

Site like Facebook and Twitter can also being used to **spread malware through messages, status updates, Likes or surveys**. This is usually in the form of a link that takes you to a site that can install malware on your computer. With the popularity of sites like Facebook and Twitter, malware spread through these social networking sites is becoming more prevalent.

File Sharing Programs

Using p2p (peer to peer) programs and networks can be a great way for you to share your files, but malware can be hidden inside files that may appear to be something you actually want**. Use extreme caution when downloading software with a file sharing program** and if at all consider obtaining software from other sources.

Pirated Software

Sites exists on the internet that offer illegally pirated software for download. These sites called warez sites, as with p2p networks, can contain software that claims to be something it is not, tricking individuals into downloading malware. **Pirated software should be avoided** anyway, besides the fact that it is illegal, the chance of being infected with malware should convince you to look at other ways to get programs.

Fake Security Popups

Fake security warnings can sometimes look like a real notification or a warning that a computer has a virus, and is another way users are tricked into installing malware. These popups can be fake security warnings with convincing suggestions that you should click and have your computer cleaned.

Being concerned about security and thinking that the anti-virus program is alerting them of a problem, many people will click on that warning. These fake warnings look real, but there are some giveaways that the computer savvy may catch. Malware creators know that most people are not computer experts and that if something that looks real, many people will believe that it is real. Sometimes though, even computer professionals fall victim.

If you are unsure if the warning is coming from your security program, **don't click anything in the box and just try to close it**. But you have to be careful here too, because sometimes the "Close" X is fake also and clicking it just installs the malware or is just a link to a bad website. Furthermore in some cases by the time you see the warning you already have malware, so **running a scan with a real and reputable virus scanner** would be a good thing to do at this point.

Avoiding all this is takes a little more effort and control. **Become familiar with your security program and any alerts or warnings that it creates**. That way, when something fake comes along you will know it is not your security program and probably an attempt to get you to install malware. If you still aren't sure what security program you have or if you have one at all, resist clicking any security warnings you see until you gain understanding of what legitimate warnings look like.

Free Games, Screensaver, or Themes

Free games, screensavers, or themes can sometimes contain slightly less evil forms of malware called **adware and spyware**. This type of malware **creates advertising popups, change your homepage and can add toolbars to your browser**. Your computer can become slow and unstable and you'll have a bad time. While these types of programs and creators aren't necessarily criminal, and the effects aren't as dire as other types of malware, you still do not want this on your computer. Aside from attempting to sell the products in the popups or the hijacked homepage, this type of malware can collect data about what sites you visit, then send that data to marketers who then send you targeted advertisements.

USB Drives

This is less common but can be just as harmful as other methods of distributing malware. USB memory sticks are everywhere and seem to be a fairly harmless device. However a USB drive with a malware payload can be inserted into your computer and the malware will install. If your computer is in a public location someone could silently insert the USB drive and install a program that would give them remote access.

Volcano.net User Guide - Malware Help

Staying Safe

As talked about in the Spam section, you are your own best protection against malware. Use caution and common sense. Install a security program to protect your computer. Here are some basic guidelines to follow.

Attachments

Don't open attachments unless either you have requested it or you can confirm from the sender that they meant to send that attachment.

Email Links

Do not click on any links in an email you are not expecting. This may be a phishing attempt to steal personal information from you. Don't get hooked.

File Sharing Programs and Sites

Avoid common sources of malware by **staying away from file sharing programs, pirated software and web sites that may spread malware**. Download files only from trusted sources.

Protect Yourself

- Use caution with email attachments and links.
- Avoid file sharing and pirated software
- Install a security program and keep it updated
- Keep your operating system updated
- Backup your computer
- Keep your computer in sight in public

Security Programs

Install a security program and learn it works and what its alerts and notifications look like. Make sure you keep your security program updated to protect against the latest threats.

Keep your Operating System updated

Make sure you have installed the latest security updates on your computer to avoid leaving your computer vulnerable.

Backup important files

Computers infected with malware will sometimes need to have its hard drive reformatted and operating system reinstalled to get rid of the problem. Without a backup all your files and documents could be lost.

Keep a good eye on your computer in public locations

Someone doesn't have to steal your computer to steal everything inside. Avoid being slipped a dirty USB.

Treat any unsolicited email, messages, or popups with suspicion

If you see anything unexpected show up on your computer, stop and count to 3 before clicking or opening. Try and remember the people who are sending all this are expecting you to act right away out of habit, curiosity, fear and lack of knowledge.

You can protect yourself by installing security software, by understanding how you can get malware, and by making good decisions when confronted with a possible malware threat. Technical solutions like installing a security program are a good idea, but you cannot just install and forget about security. For instance, security updates often come after a vulnerability has been exposed, so even if you keep your security program updated, there may be new threats out there that your program doesn't know about. You must keep alert while online. One thing malware can't make you do, is move your finger to click the mouse button.

I Think I have Malware. What Do I Do?

If you believe your computer has malware installed you should to run a scan with security software and attempt to remove the malware. **Update your security software, run the scan, and follow the recommended steps if malware is found**. Unfortunately this will not always completely remove the virus or trojan you might have, and more in depth steps will be needed. If you are comfortable with taking these advanced steps, we'll give some advice, but if not, taking your computer to a specialist would be appropriate at this time.

Advanced Malware Troubleshooting

Safe Mode - If you are running Windows, start in Safe Mode and scan with security programs. Safe Mode is a minimal version of Windows where only basic components load. Often this avoids the malware code from being run and gives your scanner a better chance of removing the malware. Press and hold the F8 key right after starting the computer to start the safe mode menu.

Forums and Specialized Tools - Security forums are good places to go for removal information, where you can post your specific problem and get direct help from a moderator or volunteer. Use caution here and verify the tools you might be using are safe and the removal instructions are appropriate. This takes some advanced knowledge of computers, so only take these steps if you are confident in your computer skills.

Advanced Malware Troubleshooting

- Ran scan with security software
- Start in safe mode and run scan
- Forums and Specialized Tools
- Scan operating system offline
- Reinstall operating system

There are malware removal tools that get rid of specific pieces of malware, but should only be used when the exact malware is identified. Security programs will identify often malware, even if it doesn't completely remove it. With the malware name though, you can search for removal instructions online and use programs recommended and used by experts.

Scan the operating system drive offline - There are other tools where you can boot your computer into a temporary environment (from a Linux USB drive, or Windows-like boot CD for instance) and scan the hard drive while it is not in use. When booted normally a malware infected computer will sometimes not allow removal because of how imbedded the malware becomes. Booting from a CD or USB drive takes the infected operating system out of the equation and will sometime result in cleaning the malware.

Reinstall the Operating System - If you have reached this point, hopefully you have backups of important files. Sometimes, to fully remove malware, the hard drive needs to be formatted and the operating system reinstalled. This step removes all data and files from the computer and unless you are a computer forensics expert, this data is unrecoverable. This is why it is important to backup your files to a location away from your operating system. This could be as simple as copying files to a USB drive, or backups could be done with a cloud service where backups are stored online. The method of backup is your choice, but any backup is better than no backup.