Computer virus examples pdf

Aaron Parsons Even on a computer with antivirus software, viruses and other malware can slip by and affect how your system works. If your computer starts behaving strangely, slows down or pops up unfamiliar programs or messages, you should start a full virus scan, even if your antivirus program hasn't alerted you to the problem. All computers slow down over time as you install more programs, but a sudden, serious, prolonged slowdown can indicate a virus. Whether it's slowing down during downloads, when programs open, or while you're waiting to download websites, this can be due to a virus that hijacks your machine's computing power or Internet bandwidth. The program, sometimes frozen or computer fails, does not necessarily indicate a virus - most of these errors are due to a software buggy. However, if the computer hangs or cuts off several times a day, or accidents start to occur in various programs, the virus may be to blame. Viruses can cause catalyses by altering or deleting the necessary system files. If the virus scan is empty, your frequent accidents may indicate a hardware failure, not a. It's normal for a hard drive to sometimes process data even if you're not using a computer, but if your hard drive keeps churning out for hours at a time, the virus can be triggered in the background. Viruses that use the processing power of your CPU can cause your computer's fan to run loudly continuously. To check the use of the processor, click the right task button and click the Task Manager button. Click More if you don't see tabs in the task manager window, then check the CPU percentage. If that number stays elevated for a few minutes - more than 20 percent without running programs - you may have a virus. Programs that can't get out properly can also cause high CPU usage, which can be solved by restarting or selecting them and pressing the End of the Task button. Many websites use ads legitimately, but if you suddenly see an increase in ads, or if ads appear rather than you browse the web, you may have a virus. Viruses can also appear as unfamiliar programs that appear in taskbars or work when you download a computer. In most cases, these symptoms point to advertising - unwanted but not malware - rather than a real virus, but some may also behave like viruses affecting your computer performance or hijacking your web browser. If your antivirus software doesn't detect these programs, install and run antivirus software The information in this article relates to Windows 8. This may vary slightly or significantly with other versions. Updated: 06/30/2020 by Computer Hope As a computer virus is the only code it cannot physically damage computer equipment. However, it can create scenarios where computer-controlled hardware is damaged. For example, a virus can instruct a computer to turn off cooling fans, causing causing computer to overheat and damage your equipment. The vast majority of computer viruses are only for targeted computer data. In addition, modern equipment is much more difficult to damage equipment without repair. If you're having problems with a computer hardware device, such as a printer, graphics card, sound card, or other hardware device, it's probably not because of a virus. Corrupt drivers Although the virus cannot attack hardware, software drivers that allow hardware devices to communicate with the computer can be attacked or damaged. If this happens, it may interfere with the device, but it will not physically damage the hardware. Keep in mind, however, that it is much more likely that drivers themselves have problems, or other software damaged drivers rather than a virus. To fix this type of problem, you need to reinstall the hardware drivers. How to install and update your computer driver. A list of computer drivers. Corrupt BIOS One of the most notable viruses that attacked the hardware was the Chernobyl virus. The Chernobyl virus was first detected in 1999 and damaged data on the hard drive and sometimes the motherboard of BIOS. When a BIOS computer becomes damaged, it causes the computer not to load. However, this virus does not physically damage BIOS; this only corrupts the BIOS code, and if the BIOS chip has been replaced, the computer will load again. Modern computers also use EEPROM, allowing BIOS and firmware to be re-flared without the need to replace the chip. Thus, if the virus infects modern BIOS, it may be re-flared with updated BIOS. Help with bios update. What about Stuxnet? Complex viruses, such as Stuxnet, are designed to damage equipment that is controlled by computers. For example, Stuxnet was designed to accommodate centrifuges in Iranian enrichment plants. No computer equipment was damaged; however, the virus damaged the centrifuges because it disabled all system alerts that would have alerted something wrong. This type of virus was able to damage equipment because security measures were disabled. However, it was one of the most complex viruses ever written and was targeted at a specific device. If your computer had contracted Stuxnet, it would have done nothing for your computer. What about PDoS? PDoS (permanent denial of service) attack is not a virus, but a type of attack where a person uses a firmware network equipment, flashing it with malicious code. These attacks can damage hardware if the firmware is programmed to do something malicious (such as disabling temperature monitors) or make the devices not work because Damaged. Why a virus writer may not want to attack the hardware of someone who creates a virus is more likely to create a virus for money, spy, or take control of a computer. Trying to write a virus virus damage to equipment does not help achieve any of these goals, nor does it help the virus spread to other computers. Note that it is likely that someone may write malware designed for the target person or company to damage the hardware. However, for this type of attack, a person will not create a virus that infects other computers. In addition, modern equipment is more difficult to damage equipment beyond repair. Today, systems use firmware that can be re-flared or reset without replacing any chip or other equipment. In addition, modern systems have security measures that help protect equipment from damage. For example, if the system gets too hot, it may shut down to prevent damage. Can the virus cause a computer to explode or catch fire? Lol there are many stories floating around that virus can cause the computer to explode or catch fire; they are invalid. Malware can damage or explode computer-controlled equipment (for example, Stuxnet destroys centrifuges). However, this will only be possible if the management software can force the hardware to do something dangerous and it will be necessary to disable any warning or prevention systems. The software can damage computer hardware. In addition, in some rare situations, adjusting these settings incorrectly can even damage the hardware. However, these program settings are not computer viruses, and as mentioned earlier, modern systems are also designed to protect equipment if it reaches a critical point. More information When viruses infect personal computers, most people will shell out $100 in McAfee to just make it go away. But why let the bloated antivirus app have all the fun and all your money? For the adventures of DIY virus fighter comes a mini firewall to keep your computer connected to the Internet, but is safely isolated from your local network, so you can freely study dangerous infections on your machine. A mini firewall called Isowall is essentially a diagnostic tool to analyze how your computer is mistakenly trying to poke on a local network. As creator Robert Graham explains in his blog, a mini firewall called Isowall is largely a tool for paranoid, but it's better to be confident than to inadvertently infect your network. Graham Isowall installation from his blog: How you See, the laptop has a direct Ethernet link to the Raspberry Pi running isowall (short purple cable for white USB Ethernet), which then links to the rest of my home network (grey cable). Photo Robert GrahamIsowall uses an external processor to run interference between a (possibly infected) computer and your home network-Graham used a Linux-equipped Raspberry Pi, but nothing with an OS that supports libpcap libpcap the library to capture network traffic should work. The machine has to be configured with three network interfaces - the first, as usual, with the TCP/IP stack SSH to it, and the other two completely empty (no TCP/IP stacks, no IP addresses-nothing). Limit the process to IPv4 and ARP packages, set the appropriate conditions for incoming/outgoing packages (found on the GitHub Isowall page) and run them. As Graham explains on the Github page: Security depends on the fact that there is no IP stack associated with adapters. This means that the infected target function cannot affect the firewall machine in any way, unless it is permitted is_allowed () function. This feature represents most of the attack surface for the firewall machine. And as you can tell from the reading feature, it contains almost no functionality, meaning that the surface of the attack is very small indeed. While Graham admits that his solution won't offer 100% security, it's refreshing to see a programmer give us a relatively easy way to play a doctor on infected machines. Not long ago, I outlined a few steps in this article on how to protect yourself from the virus if you decide not to run antivirus software in your system. However, let's say that you have followed all these steps as a good person and you will still end up getting infected, as you will probably notice once the antivirus tool you have never installed suddenly tells you that your computer is about to self-destruct. Well, that's just great. So how do you remove such a virus from your computer? There is hope and solutions. So, read on. Use Microsoft Safety Scanner Microsoft offers a tool that can remove certain types of malicious software. This tool used to be a tool for removing malicious Windows software, but microsoft has recently been offering a Microsoft security scanner. This scanner should check your computer for viruses, spyware and other bad things and remove it. There are many other similar online scanners, but some of them may cause you to actually download more malware on your system rather than delete it. Using the Microsoft tool, you can be sure that it really wants to remove any malware from your system. Install antivirus software While you probably should have installed it before using it in real-time protection, it may be helpful to install an antivirus tool now to help remove malware that is currently wreaking havoc on your system. The antivirus tool can also scan for any other files that have dormant viruses in them, waiting for you to activate them. There are many which are very effective, such as AVG, Microsoft Security Essentials, and Avast, just to name a few. These tools will hopefully be able to remove this pesky virus before it does too much harm. Search the Internet for possible solutions, although it is not recommended to use the Internet when when know that you are infected with the virus (as the virus can potentially start sending out any information it finds in your system), you can use a clean system to go online and search for a virus that you may have (based on the symptoms your computer is experiencing) and how you can remove it. If you're lucky, you can find a solution that has been tested and tested for work. Reinstall Windows Last, but not least if everything else fails, reinstall Windows or go to any other operating system such as Linux. If the virus is really that pesky, then it's best to just help Windows destroy itself so you can recover on the ashes. Before you start reinstalling, don't forget to back up your data. Please scan all the files that you back up, so you don't accidentally save the virus you're trying to get rid of and then re-infect yourself later. It's a long and arduous process, and so it's the ultimate last resort, but at least this method works every time. Don't buy a new computer! I came across enough people who think that if their computer gets infected with a virus, the world will end and they should reset the infected computer and buy a new one. This is completely untrue, as the equipment is still fine in time. Reinstall Windows as a reset system, and gets rid of the virus in the process. There's no need to go out and spend $400 for a decent new computer just because you've contracted a virus. Finding How to get rid of the virus is sometimes easy and sometimes very difficult. Your success rate will vary depending on the error you managed to catch. However, there is always one way or another to get rid of the virus. We just hope it doesn't have to be very damaging to your own data. Just remember, when it comes to viruses and protection, it is better to be safe than sorry. What's the worst virus you've managed to catch? What other tips would you add to this article? Let us know in the comments! Image Credit: AJC1 How to Clean Your Windows Computer: The Ultimate Windows Cleanup Checklist can yield huge performance improvements. Here's the final checklist for cleaning your Windows computer. Related Topics of Windows SpyWare Anti-Malware About Author Danny Stieben (488 articles published) Read more from Danny Stieben Stieben computer virus examples 2018. computer virus examples code. computer virus examples pdf. zombie computer virus examples. trojan horse computer virus examples. worms computer virus examples. examples of computer virus and antivirus. 10 examples of computer virus