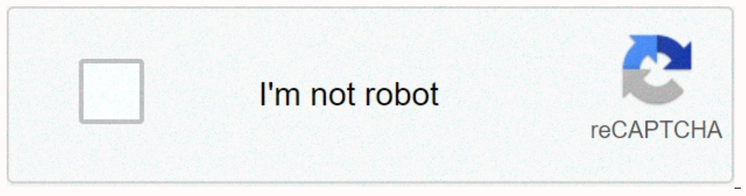

Continue

Zombie tsunami online pc

Chile's 8.8 magnitude earthquake has left its trail of devastation in Chile and an overhanging tsunami in the Pacific Ocean. Weblog Mashable rounds up several options to keep the latest news with real-time web resources. Pete Cashmore offers several real-time sources to catch up on what's happening with the tsunami, including a live video coverage page via Ustream, Twitter #tsunami hashtag, real-time results from Google and the National Oceanic and Atmospheric Administration (NOAA) Warning Center. Do you know of a better resource when affected or affected parties can adhere to the latest news and warnings? Share it in the comments. How To: Tracking Hawaii Tsunami Alerts Online [Mashable] The latest generation of video game consoles has features that use the Internet to improve gameplay. Also, many of the same games are available on PC and consoles. We compare the pros and cons of playing online games on pc vs. playing consoles to help you decide which platform you prefer. In late 2002, Sony, Microsoft and Nintendo introduced online capabilities for PlayStation 2, Xbox and GameCube. Online console games are now common with services such as Microsoft Xbox Live and PlayStation Now leading. Several titles can be played on different platforms, such as Final Fantasy XV, in which PlayStation 4, Xbox One and PC users explore the same online world. However, computers offer the largest selection of online games. Some of the most popular MMO games, such as World of Warcraft, are exclusive to PC. While PC gamers have more options when it comes to graphics cards and custom controllers, these bells and whistles come with cash costs. The main advantage of consoles over computers is price. Most consoles sell for under $500 and are often bundled with games, controllers and other accessories. A computer that is suitable for playing the latest games can easily cost twice as much. While computers have come down with the price over the years, computers are expensive compared to consoles. There are ways to save on a PC, but it's not easy to get the pc price to a price comparable to the most expensive console. As your computer gets older, there's a reasonable chance it'il extend the life of games with a component upgrade. When the components in the console are dated, there is usually no way to solve the problem without replacing the entire console. In most cases, upgrades that could prolong the life of the system are not an option. One of the biggest advantages that computers have over consoles is that there are more games, especially when it comes to multiplayer online games. The majority of MMOs are designed for PC. PC gamers have the ability to play MUD, email games, browser games and titles that are digitally distributed or available as free downloads. If you want to change the game files or create computer is essential. Computers are always on the cutting edge of gaming games The current generation of high-resolution consoles briefly narrowed the gap. Still, well-equipped computers continue to offer superb graphics. High-resolution monitors and the latest multicore processors and dual graphics solutions allow you to build a powerful gaming system. Even if a console offers amazing technology at its launch, there is no way to compete with rapid hardware advances in the computer industry. Multiplayer games are facilitated with companies like Microsoft and Sony offering online services for their products. Consoles come equipped with a network card, making it easy to connect to the Internet and get into a multiplayer game. The games console tends to have a lower learning curve than computer games because of the controls. You may need quick thumbs up, but you usually don't have to spend hours in a lesson that teaches how to work with basic features of the game. Configuring graphics, login, and network settings for computer games can be a technical nightmare. On the other hand, you can take a console home and play a game within minutes. There is no operating system to configure or update drivers, and there's no accident you'll buy games that your console isn't powerful enough to run. Consoles perform one task well. In contrast, computers can be used for a wide range of tasks and entertainment. Some console manufacturers try to make their systems flexible. However, it is doubtful that consoles will support the variety of apps that are available for PCs. When it comes to online games, computers offer different ways to connect to the Internet and other computers that are not limited to their own services or software. Different brands of computers and operating systems usually communicate well with each other. There is a clear lack of interconnection between different console brands. Many games are available for one type of console, but not for others. When it comes to online play, everyone is usually limited to their network. This means that people with Xbox consoles can usually only play against other people with Xbox consoles (although there are some exceptions). There are many things to consider before choosing a gaming platform. The most important among them is to decide which games you want to play, how much money you want to spend, and whether you need a computer for other purposes. Having both is perfect. However, if you're new to the world of online gaming, it might be best to start with a console due to lower costs and simplified setup. If you are a hardcore gamer who wants to play as many online games as possible, then consider a special computer for games. Thank you for informing us! Tell us why! It's something to make your blood get cold. You just closed Microsoft Outlook when your system suddenly without warning. When Windows goes back, everything seems normal, but then you notice... Changes. The Internet Explorer home page may be different, or certain websites may not load at all. at all. unusual disk action or inexplicable mouse stillness. Congratulations, your computer has just been hijacked. In the time it takes to look at a JPEG image on a web page, your computer may fall victim to a insidious attack that turns computers into mindless unmanned drones dedicated to performing malicious actions on behalf of remote hosts. In the past, infected computers, known as zombies, would receive instructions to send a blizzard of data to a specific web address or Internet server. Called distributed denial of attack, these infections have taken hundreds or even thousands of computers to download even the best entrenched servers and websites. If your computer looks tucked, if your hard drive rotates when you don't sign in, or if your Internet connection is active when it shouldn't be, you may have a zombie COMPUTER on your hands. The best-case scenario is that it will simply affect the way your system works; in the worst case, your system is inadvertently used to launch attacks that can be traced to you. Either way, see the accompanying article, Zombie Repellant, to learn how to protect yourself. Over the past six months, zombie networks have become something more capable and dangerous - so-called botnets, which is short for robot networks. Like zombie computers, botnet systems are infected with a virus that allows a remote server to command them via an Internet connection. But when zombie computers perform one task - flooding a target with bits - the systems in the botnet are dynamic. They can be programmed and updated to engage in all kinds of malicious actions. I think it's really an indicator of the originators of these threats that are becoming more sophisticated, says Oliver Friedrichs, senior manager for Symantic Security Response. Today, these bots tend to be used for more two-faced purposes, such as phishing attacks and spam in general. Attacks not only become more sophisticated, but also increase at an alarming rate. The Symantec report on internet security threats revealed in September that the number of active bot systems on the internet has skywarded from 2,000 systems in January 2004 to 30,000 systems in June. Organizations like the Internet Storm Center at the SANS Institute make new botnets open almost every day. Unfortunately, it becomes more difficult and harder not to turn out to be an unwitting accomplice of a zombie PC attack. Symantec warns that the time between detecting a vulnerability in your computer's security software and when an attacker sees a virus to take advantage of this vulnerability is less than six days. Some software companies that remain unnamed can take weeks or months to patch their products. Perhaps most confusing is the changing form of the threat. Botnets are used for financial gain - driving junk mail offers that allow phishing scams that lure disclose personal information and capture financial and account accounts pressing keys and other techniques. The botnets are even hired as blackmailers. Internet gambling house Blue Square suffered a massive distributed denial of service attack earlier this year after failing to respond to an email demand for money. Much of this activity comes from Eastern Europe, far beyond the reach of U.S. regulators and law enforcement. There is a much more insidious and criminal aspect to these bots than there has been in the past, Friedrichs says. Over the past few decades, viruses and worms have not been written for monetary gain. We are now seeing new types of attacks that are clear to a much more insidious mind, in terms of getting financial details, bank account information and usernames and passwords for financial institutions. In fact, the proven effectiveness of botnets has helped create a healthy black market for infected machines, Friedrichs says. We're starting to hear that the people who are deploying these botnets are actually selling them. So if I deploy a botnet several thousand systems, someone will be ready to buy it from me. Now there really is an incentive to deploy botnets. What is the value of a network of compromised machines? Spammers use botnets to send millions of email messages from thousands of computers around the world without fear of detection. And because spam originates from so many different points, IT is difficult for ISPs to cut off the flow of unsolicited traffic. Eventually, users can find their email rights that are revoked after bot processing software triggers outgoing data. But this leaves ISPs no closer to shutting down an intruder spam server or other computers in a botnet. Matt Neyley, an independent security consultant from Myscatoix, has seen more than his share of botnet-related infections and exploits. His concern is that the open nature of botnet infections - allowing updated viral software to be downloaded to a computer at any time - makes system recovery difficult or even impossible. The most important thing about bots is after I call home, you really do not know what he has done to your system. And finding out what's been done can be very difficult, Elli says. The approach I've taken has used Windows Recovery --if you know when the infection occurred, you can go back beyond that moment. But there comes a time when you have to say that so much damage has been done that it is best to start over. Even finding out if your COMPUTER is infected can be difficult, Egi says. He points out that botnet virus writers can monitor the antivirus provider's websites to see if their latest exploit was addressed with an updated viral signature. Authors can then tweak the existing virus code and test it on popular antivirus programs until they come up with which may slip from undetected. From there, it's just a matter of transmitting the updated code to the active botnet. These threats have become better in terms of hiding in your system, friedrich says. They can disguise themselves as different software. They can hide in a running service. What can you do? It's best not to get infected. This means that you run antivirus software, anti-spyware, and firewall. Firewall software that monitors outbound traffic can warn you that your computer is bad. In addition, make sure your system is patchy and up-to-date, as many botnet exploits rely on flaws in Windows, Internet Explorer, and other popular software to get into your system. With the right precautions, a zombie PC won't look as scary as a goblin on the front door. Michael Desmond is a freelance writer who lives in Burlington, Vermont. It has a whole new appreciation of the challenge that antivirus companies face. Note: When you purchase something after clicking on links in our articles, we may get a small commission. Read our affiliate link policy for more details. Details.