

September Newsletter

Don't Hold Your Breath Computer Service

If you have any suggestions, or questions for our monthly newsletter please e-mail them to decker_brian@computerbreath.com.

Alerts:

Sony

Sony Corp. has launched a voluntary recall of 438,000 Vaio portable computers, citing a potential hazard that could cause the machines to overheat or possibly burn a user. Sony's recall affects 72,800 computers in the United States. The flaw, in Sony's VGN-TZ100, VGN-TZ200, VGN-TZ300 and VGN-TZ2000 series computers, the recall is related to "irregularly positioned wires near the computer's hinge and/or dislodged screw inside the hinge" that can cause a short circuit and overheat, the agency said. "This poses a burn hazard to consumers," the agency added. "Sony has initiated a voluntary program to perform a free inspection and, if necessary, a repair to ensure these units meet our high quality standards."

Microsoft Updates

Microsoft plans to issue four major security patches all deemed critical meaning that the vulnerabilities could allow an attacker to remotely install malicious code on a user's PC without any user intervention or consent. Often users will be enticed to open a malicious link or visit a harmful Web page through some type of sophisticated social engineering scheme delivered via e-mail. Fixes for these vulnerabilities in Windows is scheduled for today at approximately 1 p.m. The patch which is labeled "Windows Bulletin" promises to be a massive update, fixing multiple Windows bugs in IE, and several operating system errors on XP and Vista as well as glitches in Microsoft .net Framework, Microsoft Office, Digital Image Suite, Visual Studio, Visual Fox Pro, Forefront Client Security, Windows Server 2003 and Windows Server 2008.

Hotmail

Microsoft is warning Windows Live Hotmail users of a recent phishing scam that asks for the person's username, password, date of birth, and country or territory. It's not clear why the software giant has taken the time to warn users of this particular phishing scam, as this definitely isn't the first Microsoft- or Hotmail-related one. Hopefully, it has nothing to do with its success rate, but it's likely due to the fact that the e-mail claims it is from the Windows Live Hotmail team, both in the signature and at the start: "This Email is from Hotmail Customer Care and we are sending it to every Hotmail Email User Accounts Owner for safety."

Hackers

Hackers have broken into the corporate databases for Best Western Hotels and may have stolen the names, addresses and credit card information of every customer who stayed

with the international group since 2007. If you stayed at one you may want to keep a watch on your credit

Microsoft warns of IE8 lock-in with XP SP3

Microsoft yesterday warned users of Windows XP Service Pack 3 (SP3) that they won't be able to uninstall either the service pack or Internet Explorer 8 (IE8) under some circumstances. The warning was reminiscent of one Microsoft made in May, when Windows XP SP3 had just been made available for downloading. At the time, the company told users they wouldn't be able to downgrade from IE7 to the older IE6 browser without uninstalling the service pack.

Computer World In August:

Comcast

Comcast, the largest provider of cable-based broadband service in the U.S., will limit residential customers to 250GB of bandwidth a month beginning Oct. 1, 2008. Comcast will contact customers who go above the 250GB limit and ask them to curtail their use, Comcast said. If a customer goes over the monthly limit again during the following six months, Comcast will suspend service for a year. Currently, Comcast contacts high-bandwidth customers and will suspend their accounts if they don't curb their use, but it has not set a firm bandwidth limit until now. Most customers contacted about their bandwidth usage agree to limit their activity, according to Charlie Douglas, Comcast's director of communications. Earlier this month, the U.S. Federal Communications Commission struck down Comcast's past network management practice of slowing BitTorrent peer-to-peer traffic in an effort to reduce congestion. The FCC ruled that Comcast was violating so-called net neutrality principles by targeting a certain kind of Internet traffic. The new bandwidth cap will affect less than 1 percent of Comcast customers, Douglas said. Those customers "are using so much bandwidth that they are degrading the experience of other users," he added. "Two-hundred-and-fifty gigabytes are an extremely large amount of data." Some high-bandwidth users have asked Comcast to identify a specific cap so they know where the line is, Douglas added. Some other broadband providers also warn customers about excessive bandwidth use.

An average Comcast customer uses two to three gigabytes of bandwidth a month, Comcast said. To reach the 250GB limit, a customer would have to do one of the following: send 50 million e-mails, download 62,500 songs, or download 125 standard-definition movies, the company said in its announcement. Comcast has also looked at charging high-bandwidth users additional fees, and it still has not ruled out doing so in the future, Douglas said. Comcast is also looking at "de-prioritizing" heavy users' traffic during times of network congestion. The plan Comcast is considering would slow heavy users' traffic for up to 20 minutes during times of the most congestion.

Comcast will notify customers of the new bandwidth limits using several methods, including banner ads at Comcast.net and notices sent with monthly bills, the company said. Some net neutrality advocates criticized Comcast for not telling customers of its previous network management plan to slow P-to-P traffic at times.

Some net neutrality advocates have said Comcast's new network management plan of targeting an individual user is preferable to blocking Web applications. But others have suggested that those efforts may be equal to penalizing their best customers. See more at the end by Steve French

Google Chrome Web Browser

The browser is designed to be lightweight and fast, and to cope with the next generation of web applications that rely on graphics and multimedia. Called Chrome, it will launch as a beta for Windows machines in 100 countries, with Mac and Linux versions to come. The new browser will help Google take advantage of developments it is pushing online in rich web applications that are challenging traditional desktop programs. Google has a suite of web apps, such as Documents, Picasa and Maps which offer functionality that is beginning to replace offline software.

Largest ID theft case ever!

Federal prosecutors are gearing up for what they believe will be the biggest identity theft prosecution in U.S. history, after investigators broke up a major hacking ring allegedly responsible for stealing and selling more than 40 million credit and debit card numbers. Hacking into wireless computer networks of several major corporations, including OfficeMax, Barnes & Noble, Boston Market, Sports Authority, Forever 21, DSW, BJ's Wholesale Club and TJX Companies, which operates retail stores T.J. Maxx and Marshall's.. They used sophisticated computer hacking techniques that would allow them to breach security systems and then install computer programs that gathered enormous quantities of personal financial data, which they then allegedly either sold to others or used themselves.

Private browsing feature in Internet Explorer

One of the most interesting feature that didn't quite make it into the final release of Firefox 3 is "Private Browsing", a.k.a. porn mode. The only other browser with this feature built-in today is Safari, however, Microsoft may also be building a similar feature into Internet Explorer 8 if two trademark filings are any indications. Although "private browsing" can be easily associated with viewing particular genres of media content, the Mozilla foundation argues "while viewing pornography may be a popular use case due to the nature of content on the Web, assuming that this is the only reason that users need private browsing trivializes the overall feature. For instance, users may wish to begin a private browsing session to research a medical condition, or plan a surprise vacation or birthday party for a loved one." If indeed Microsoft is rolling out such a feature in Internet Explorer 8, I can imagine it becoming very popular with surprise birthday planners across the world. Oh those birthday people are in for a treat.

Is your computer a Zombie

The number of compromised zombie PCs in botnet networks has quadrupled over the last three months, according to figures from the Shadowserver Foundation. Shadowserver tracks botnet activity and the number of command and control servers. It uses a variety of metrics to slice and dice its figures based in part on the entropy of botnet infections. The clear trend within these figures is upwards, with a rise in botnet numbers

of 100,000 to 400,000 (if 30 day entropy is factored into equations) or from 20,000 to 60,000 (for five day entropy).

Entropy of botnets is calculated on the basis that if no activity is seen from a specific IP for a number of days - either 30, 10 or five - then it is removed from the botnet count.

Shadowserver figures suggest the number of command and control servers has actually decreased over the last month, following a spike in activity back in July.

Security watchers at the Internet Storm Centre have a number of explanations for the rise in the zombie population.

It could be that experienced botnet herders have got better at keeping control of compromised machines, or that more machines have been infected. Not much by way of email malware activity has been monitored, so if the latter explanation is true, then drive-by download attacks are playing a bigger role in spreading botnet client infestation. The recent rise in SQL injection attacks that plant malicious scripts on vulnerable servers could be to blame, but there's no hard data to support this plausible theory.

Improved detection of web-based attacks may be needed to gauge the extent of the problem, according to security watchers at the Internet Storm Centre.

"We are very good at tracking email-based malware (including lead-the-user-to-the-bad-website variety) and certainly network based attacks," writes ISC staffer John Bambenek. "Short of spidering the web on a consistent basis, it gets difficult to find infected sites for that malware. We at the ISC, and I'm sure many others, are working on ways to honeypot pure web-based attacks to capture this malware, but much work is left to be done."

Data Bits:

Most Users Share Personal Data Online

Although 84 percent of internet users claim they never give out personal details online, the reality is very different, says AOL. According to research conducted by the web portal, 89 percent of internet users have at some point willingly given away personal details online, highlighting that while surfers may understand the dangers of data security online, they don't actually take steps to ensure their safety. The results of the survey also show that 34 percent of Web users expect to be the victim of credit card fraud online, while only 11 percent have actually experienced the problem.

Driving Under the Influence of Technology

During a survey of Americans, Findlaw.com found that drivers between the age of 18-24 where more likely to have sent a text message, an instant message or e-mail while driving. In the age group of 25-34, almost 27 percent admitted to these dangerous driving behaviors

Spam

The Center for American Progress and the Center for Democracy and Technology have released a report which shows in 2007 "the FTC reported 221,226 internet-related fraud complaints, up from almost 16,000 in 2006 and more than 24,000 from 2005."

Odd News:

Google's Street View

A man who fell asleep in a drunken stupor on the grass outside his home was horrified to find his embarrassment posted on the internet. He had been drowning his sorrows over the death of a friend and collapsed after climbing out of a taxi. As he slept off his excesses, a car-mounted video camera passed by to record pictures of the street for Google's StreetView website. Within days a photographic record of the neighbourhood and its unusual presence was available for worldwide viewing.

Random Thoughts from DHYB consultant Steve French:

Your access to the Internet is under attack! Do you remember in the 1990s that big communication companies like AT&T and Comcast said they had to raise rates because they needed the money to upgrade their infrastructure to Fiber Optic to provide increased capacity for High Speed Internet? "Half of the nation's households are not connected to broadband, and the United States is falling far behind other developed nations in broadband speed, price and availability. We pay far more for a lot less bandwidth than our global competitors -- and we lack enough competitive choices in the market to push speeds up and prices down." (Freepress.net) So, if we have already been paying for increased capacity (bandwidth) why is Comcast trying to LIMIT your access to the internet in what appears to be a direct violation of an FCC ruling? Oh, sure they're appealing the decision, no surprise there, but they have also announced that they intend to go ahead and limit YOUR ability to download from the Internet anyway.

Net Neutrality is a big subject with lots of ups and downs, pros and cons. This is how I see the issue:

This is only the first round of the big company's attempts to charge you more for the Internet. If allowed to become the Internet's "Gatekeepers" these companies will decide FOR you what you can access over the Internet. Know what this access decision will be based on? You're RIGHT! Money. Not only will YOU pay more for access but what sites you can visit will depend on how much money the Site Pays as well. So if you have your own Web site for family members to share pictures with each other you will have to PAY your ISP (Internet Service Provider) for access to the Internet, PAY for the site itself, and PAY so that it can even be seen by your family who will also have to PAY to be able to see your site. You and they will literally have to pay, and Pay, and PAY!

But wait! There's MORE!!! Let's look into my Crystal Ball and take a look at what the future of the Internet looks like. I see an Internet that is structured almost exactly like Cable TV is today. Basic, Expanded, and Premium Internet Access Packages with the company deciding for you what sites you can see and which ones you can't depending on how much money you are willing to cough up by the month. Sound Familiar? Add to this the Phone Company's way of packaging telephone service with different plans with different services and the internet becomes the sole domain of companies like Comcast and AT&T. I can see it now: Institutionalized SPAM! I have to stop looking into the Crystal Ball now, I'm scaring myself.

