

Doctors Orders

Hello and welcome to another bumper issue of Doctors Orders.

Because our new remote access support package has attracted lots of new customers from outside Northants, I thought I'd better mention what Doctors Orders is for those who've just spotted it in their inbox. (Regular readers can skip this bit).

Doctors Orders is the monthly newsletter from Computer Doctors. My name is Craig and I'm a trainee computer engineer.

I like to think that I got the job of assembling the articles from the scrappy notes the engineers give me, into the polished product that is Doctors Orders, because my journalistic skills showed through on my CV. Or maybe the raw enthusiasm of youth impressed the boss so much, after this small test maybe he is going to fast-track me into management.

Unfortunately, when I asked, he said, "Nobody else wants to do it and you work cheap".

So with my dreams shattered, lets see what goodies we have this month.

Well in amongst the usual viruses to avoid and spyware that steals your credit card numbers, there's Spotify a legal music download that won't fill your PC with spyware.

Also if you are thinking of getting a mobile Internet dongle, don't do it until you've read how to get a free laptop as part of the deal.

But the best bit is not in this month's newsletter at all!

The powers that be are organising a competition to win a free computer package. The kit didn't arrive in time so we've had to postpone it until next month. So don't miss next months exiting episode.

Don't think you won't win either, because it's not like the lottery where there are millions competing. This is just for our customers and their friends and families, to say a big thank you for sticking with us through these troubled times.

The drawback if you win (there's always one isn't there) is that you have to have your photo taken with the boss to put in the next newsletter. My heart goes out to you, whoever you are.

You don't have to be a computer geek to win as I am assured that all the correct answers are on our website.

So if anyone wants to make a bid for the list of correct answers, I'll be in The Cromwell Cottage in Kislingbury, on Saturday night, holding up a pint of real ale.

You'll know me, I'll be the one with the red nose!



Inside this issue

- U.S. completes first prosecution of foreign phisher
- Paul McCartney website hit by malware crooks
- British teens tempted to hack for money
- Tiscali looks next for the slippery slope
- Neeris Worm follows in Conficker's footsteps
- Dell and HP refuse to replace bad NVidia chip
- Version 2 of Firefox is no longer secure
- Wireless connection slows to a crawl
- Free Laptop with mobile Internet Dongle
- Crooks exploit Ford in scareware attack
- BBC's Botnet Attack.
- Youngsters warned of social networks' threats
- Spotify, An Alternative to Music Piracy
- Microsoft extends Red-Ring-of-Death cover to fresh Xbox fault
- Amazon refuses to be tracked by Phorm

U.S. completes first prosecution of foreign phisher

A Romanian hacker has become the first overseas national to be convicted by a US court for the crime of phishing.

The landmark case saw a 23-year-old Romanian arrested in Bulgaria and extradited to the US for setting up a number of fake banking sites, from which he then sent out thousands of fraudulent messages in a bid to trick victims into parting with sensitive information.

Following on from a lengthy case, the United States District Court in Connecticut has only now found the fraudster guilty, handing down a five-year prison sentence.

In a statement issued to the court, one victim explained: "Above all else is the helplessness, knowing that all my personal information is forever now in the public domain.

"This is a huge invasion of privacy, and as such it has caused me a great deal of anxiety."

According to Network World, computer security experts in the US now believe central and eastern Europe to be one of the biggest growth areas for online crime, with Romania and Bulgaria in particular home to thousands of online criminals.

Paul McCartney website hit by malware crooks

Former Beatle Paul McCartney's website was recently targeted by cyber crooks who compromised the online security of the site and planted malware, it has emerged.

The site was hit by "a string of website compromises", according to internet security firm Scansafe, which says the Luckysploit exploit toolkit was involved in the operation.

Spotted over last month, the LuckySploit malware, which was hidden behind an invisible iFrame on the site, works by loading banking trojans onto the computers of people visiting a website.

"As far as exploit toolkits go, Luckysploit is a bit unusual inasmuch as it uses an asymmetric key algorithm (standard RSA public/private key cryptography), to encrypt the communication session with the browser," explained the firm.

"Impacted sites may not just be spreading new Zeus banking trojans and bots, their management systems may also be infected with previous variants of Zeus bots and banking trojans."



I'll go the foot of our stairs

We are always banging on about viruses and spyware, both in our newsletter and to any customer that will listen. If I had a pound for every time I've said "Run your antivirus and anti-spyware programs every month", I'd be very, very, very, rich.

Imagine the look of horror on our faces when a new customer walked into our workshop last week with a PC that was so full of spyware, BT had closed down their Internet connection to stop the spread of spam emails and worms. When asked why they had no antivirus or anti-spyware programs installed, said the computer repair company they used previously told them they didn't need it and viruses were "overrated".

For the first time in many years, we were all unanimously speechless!

British teens tempted to hack for money

Parents in the UK have been advised to ensure they are aware what their teenage children are up to online as one in three are tempted to hack for money, according to new research.

Internet security firm Trend Micro has published figures painting a worrying online security picture showing some teens are ready to spy, hack or even steal money online.

One in seven have impersonated someone else and over four out of ten have hacked into someone else's profile, with boys being twice as likely to do so compared to girls, the research showed.

"These results come as a stark warning to parents to become a lot more familiar with what their kids get up to when online ." said Rik Ferguson, security expert at Trend Micro.

"Parents need to ensure they lead by example at all times, clearly but appropriately lay down some simple family guidelines and make sure they oversee the online activity without being obviously intrusive."

It is advisable to keep security software up-to-date and place computers in common areas to protect children online.

More reasons to postpone that upgrade to IE 8

We received some emails from readers who agree with our recommendation last month that you wait before switching from Internet Explorer 7 to the new version 8. Several people who had already taken the IE 8 plunge explained why they reverted to the earlier release. For Glen Archer, the problem was a conflict with one of his security apps:

"Soon after installing the public release of IE 8, I noticed that it was very slow to start. I've since discovered that it's not just my XP SP3 machine alone. It seems there's a conflict between IE 8 and some resident (real-time) antispyware applications that centres around these applications' restricted-zones lists and IE 8's SmartScreen security function.

"Spybot Search and Destroy and SpywareBlaster are the ones commonly mentioned, but I use SuperAntiSpyware Pro and my zones list is short. That leaves [as the cause] an add-on conflict, which I didn't check. There are some workarounds proposed until MS fixes the problem, but the easiest one — and the one I chose for now — is to go back to IE 7. That brought IE back up to speed."

Martin Davies found the source of his IE 8 conflict, but he rolled back to the previous release anyway:

"Saw the article in last months newsletter and thought you'd like to hear another reason for not rushing into IE 8 (though, after uninstalling it, I discovered a workaround). I installed IE 8 the other week, and at first things seemed OK — until attempting to add a C++ function within Visual Studio 2008 Pro, using a wizard. This resulted in a script error.

"I quickly uninstalled back to IE 7 and rebooted. The add function, etc., worked fine in VS 2008 again. A week later, I was checking the Visual C++ Team Blog and found this blog post.

<http://blogs.msdn.com/vcblog/archive/2009/03/28/some-vs2005-and-vs2008-wizards-pop-up-script-error.aspx>

That solves the problem, but you would've thought they'd have caught this one before release!"

Tiscali looks next for the slippery slope

Tiscali's attempt to sell its assets last month followed by its accountants refusal to sign off its annual accounts http://business.timesonline.co.uk/tol/business/industry_sectors/telecoms/article5874543.ece have led to speculation that it's about to go under.

In our opinion, Tiscali's only good point was its cheap price as the quality of the product was always poor. If you think that all ISP's are the same and price is the only difference, have a look at :

www.computerdoctors.uk.net/pages/bband.htm

Neeris Worm follows in Conficker's footsteps

All the media hype about Conficker unleashing some dastardly new attack on April 1 turned out to be just that: hype. Since we were pretty sure Conficker would be a non-issue on April 1, it came as no surprise when nothing much happened on that date.

In our opinion, the media would have done well simply to say "Conficker might become active on April 1, so clean your systems before that date." This is precisely the advice offered by our tech support.

The fact is, trouble can strike your systems any day, so use some common sense and don't fall victim to the scaremongers.

That said, at least one other worm is now being hyped as "Conficker's cousin." The latest rendition of the Neeris worm — which was first detected back in 2005 — is exploiting the vulnerability patched by the update described in Microsoft security bulletin MS08-067.

<http://www.microsoft.com/technet/security/Bulletin/MS08-067.msp>

That's the same hole Conficker has often exploited to spread itself.

The new Neeris variant can infect new systems by taking advantage of Windows' AutoRun feature. Once the worm makes it onto your computer — via a malicious download, infected media device, or other source — it sets itself to load every time Windows boots up. Later, if you insert a removable media device, it'll try to infect that device using the same AutoRun hole that Conficker attempts to leverage.

If a removable device becomes infected and then is inserted into a non-infected system, AutoRun — via the autorun.inf file on the infected removable device — will try to launch the code to infect that system. You'll find more information about the exploit on Microsoft's Malware Protection Centre.

<http://www.microsoft.com/security/portal/Entry.aspx?Name=Worm%3aWin32%2fNeeris.gen!C>

The infection then sends links over various chat channels and may try to copy itself onto your system's removable drives. It's also capable of hacking into SQL servers and spreading via the security hole that's fixed via MS06-040.

<http://www.microsoft.com/technet/security/Bulletin/MS06-040.msp>

What you need to know — before the media hype gets too thick — is that Neeris is no big deal. If your antivirus software is up-to-date, the worm most likely won't affect you, because your security software will detect the worm and stop it cold.

Dell and HP refuse to replace bad NVidia chip

An old urban myth claims that the microprocessors used in PCs and other consumer electronics are designed to fail within days or weeks of their warranty expiration.

For tens of thousands of people who bought Dell and HP notebooks whose motherboards fried — often a few weeks after their warranty expired — there's nothing mythical about it.

The cause of the machines' fried motherboards is an overheating NVidia graphics chip. The failure rate is so huge that NVidia in the U.S. had to take a \$196 million charge against earnings in the second quarter of its 2008 fiscal year in anticipation of the reimbursements that would result from the faulty graphics chip.

What's particularly scandalous, though, is how HP and Dell first handled the deluge of complaints from customers with notebooks that failed after their warranties expired. The companies either charged the customers (victims?) for repairs or refused service because the systems were past the warranty period.

Even worse, HP and Dell continued to sell notebooks with the same NVidia chip long after the companies were aware of the problem. (Ultimately, NVidia released a new version of the graphics chip that didn't cause overheating.)

Unwary consumers who purchased the affected notebooks — no doubt based in part on the heady reputations of the vendors — were left in the lurch when their PCs failed, which usually occurred after 18 months or so. The purchasers had no recourse except to yell and scream at clueless tech-support reps.

When the heat from consumer complaints became as hot as the faulty NVidia chip, HP and Dell relented and published a list of defective model numbers on their Web sites. Dell extended the standard one-year warranty to two years for the systems they identified as having the problem. HP offered a 24-month warranty extension for the specific issue.

However, instead of issuing a recall — as you would expect in such a clear case of a defective part — the vendors instead merely offered a BIOS upgrade. The "patch" for the affected notebooks made their fans run continuously in an attempt to lower the graphics chip-induced heat, which was cooking the motherboards onto which the chips were soldered.

This "fix" merely extended the time before the mother-

boards finally burned out while simultaneously devouring the machines' battery life. Of course, notebook purchasers became further inflamed by the power drain on their systems due to the constantly running fan.

How to get vendors to respond to your problems

There ought to be a PC lemon law, like the lemon laws enacted in the U.S. that protect purchasers of defective cars. Those laws came about because legions of consumers complained after they got stuck with cars — new and used — that were badly made. Until such protections are available, you can take the following steps to get redress for your grievances:

Post a description of your gripe on consumer-complaint blogs.

People who bought the defective HP and Dell notebooks would have been out of luck if it hadn't been for the rising power of Internet communities and blogs — ironically, some of which were on the vendor's very own sites. These grass-roots efforts demonstrate that consumers are not powerless when they own a lemon PC, even in the absence of a lemon law to back them up.

As the number of postings about the problem on gripe sites rose, HP and Dell could no longer hide from their customers. For example, the site HP Lies <http://hplies.com/viewtopic.php?f=4&t=130> was created specifically for consumers to fight back against what the site calls "HP's cover-up of the NVidia defect." A massive number of people who had bought now-dead HP notebooks that fried due to the overheated NVidia chip not only showed their displeasure at the company but also offered legal and logistical advice to others who shared their misfortune.

Surprisingly, many burned customers discovered the HP Lies site through links on HP's own Business Support Forum.

<http://forums11.itrc.hp.com/service/forums/bizsupport/questionanswer.do?admit=109447626+1239272077992+28353475&threadId=1274587>

Likewise, news of Dell's offer of a limited warranty enhancement with a list of affected units was reported at Dell's Direct2Dell user-community blog

<http://en.community.dell.com/blogs/direct2dell/archive/2008/08/18/nvidia-gpu-update-dell-to-offer-warranty-enhancement-to-all-affected-customers-worldwide.aspx>

as a response to the thermonuclear anger expressed by unhappy customers at the site.

Take it to court.

Many U.S. customers went the legal route and filed lawsuits that were consolidated into a class-action complaint against NVidia, Dell, and HP last September. While less effective in getting a full reimbursement or replacement, lawsuits serve as a wake-up call to corporations and produce corresponding action to mollify the plaintiffs.

Skip low-level tech support and go directly to the top.

If you have a PC problem that's been proven to result from a defect, ask to speak to a high-level tech-support representative, who will be more empowered to address your complaint — and likely more knowledgeable about the issue as well.

Be persistent, but keep your cool. Advice at the HP Lies site suggests going the corporate route and obtaining a case manager to get free repairs or a replacement, which standard tech support might not provide.

Buy an extended-service warranty.

HP and Dell customers who had extended warranties got no-charge repairs and/or replacements for their NVidia-murdered systems. Because cheaper components are used in most of today's low-cost computers, chances are those components will fail sooner than in the past. Extended warranties generally offer no- or low-hassle tech support and repairs for up to three years beyond the standard warranty.

Version 2 of Firefox is no longer secure

I didn't think I would ever say this, but it's time to uninstall Firefox — if you're using version 2, that is. You need to update to version 3.0.8, because Mozilla stopped supporting the older release as of last December. Version 3.0.8 is now the only secure version of the browser.

At the recent CanSecWest security conference, Firefox was one of the browsers that were compromised in a hacker contest.

The vulnerability that came to light in that contest has been patched in version 3.0.8, as Mozilla has acknowledged on the organization's security blog. <http://blog.mozilla.com/security/2009/03/26/cansecwest-2009-pwn2own-exploit-and-xsl-transform-vulnerability/>

If the latest Firefox version hasn't already been offered to you, visit the Mozilla Foundation's download page to download and install it.

<http://www.mozilla.com/en-US/>

Wireless connection slows to a crawl

"Ask the Doctor"

"I run wireless on my PC. Typically, I would get 1.5–3Mbps transfer rates to my networked storage drives. I recently went on holiday and cleaned out my home/office to have it painted while I was gone.

When I set up my PC again upon returning home, my wireless-transfer speed dropped to 512Kbps or less. Everything is set up as it was before I left, and my wireless router has not moved or been reconfigured.

Most Wi-Fi setups are designed to "fall back" to lower speeds if there's temporary interference or some other communication problem. Trouble is, they don't always revert to full speed when the interference passes, and perhaps this is what happened here.

Next time you notice your connection slow down, disable (in some routers, "disconnect") your PC's Wi-Fi link so that you're no longer connected to your access point/router. Next, physically reboot the access point: use the power switch or unplug the power cord, wait half a minute or so, and re-energize the access point. Finally, reconnect to the router by re-enabling your computer's Wi-Fi connection. Many times, that's all it takes to restore top speed after an unrecovered fall-back.

If the slowdown happens frequently or all the time, look for a new external Wi-Fi interference source, such as a portable phone, microwave oven, garage-door opener, baby monitor, or another Wi-Fi setup — perhaps even a neighbour's device.

You can sometimes avoid wireless-network slowdowns by changing the channel used by your Wi-Fi network. Many routers default to Wi-Fi channel 6 or 9, which is in the middle of the allotted radio spectrum. But Wi-Fi can operate on any of 13 standard channels. Choosing a different channel may be enough to avoid interference.

The manual that came with your access point/router should contain instructions for changing the channel. Once you've reset it, your PC's Wi-Fi adapter will find the new channel automatically; there's usually no need to change anything at the PC end of the connection.

You'll find more information on About.com's wireless-troubleshooting page.

http://compnetworking.about.com/lr/wireless_signal_interference/156388/1/

Usually, one of the two simple steps above — a cold reboot of the router and/or changing the operating channel — will get you going again.

Free Laptop with mobile Internet Dongle

You can get the much sought after Samsung NC10 Netbook absolutely free when you take a mobile Internet contract with O2.

If you prefer something more fitting for a road warrior, then the Samsung R510 will fit the bill.

Both these deals are available only while stocks last.

If they are of interest please call **Hayley Morris or Susan Coburn on 01858 410010**.

They also have very attractive deals on modem only mobile Internet. So if Broadband has not yet come to your neck of the woods and you can't wait for BT to get around to upgrading your local exchange, give them a call. If you can get a mobile phone signal you can have mobile Internet.



<Samsung NC10

From £25.53 month

Laptop FREE on 24 month contract. Includes free modem

Samsung R510 3Gb>

From £25.53 month

Laptop £68.08 on 24 month contract. Includes free modem.



Crooks exploit Ford in Scareware attack

Cyber crooks are exploiting the name of the Ford Motor Company to expose internet users to online threats with the use of search engines, an online security firm has said.

People searching for information on Ford vehicles are the target of the scareware attack, which has more than one million malicious links all targeting Ford, according to Panda Security.

The attacks work by tricking search engines to inadvertently promote the malicious pages to the top of rankings when the relevant search terms are entered.

"Once the user visits one of the malicious sites, they are prompted to download and install a malicious "codec", which then installs the MS AntiSpyware 2009 (softwarefortubevie.40030.exe) rogue security software," said Panda.

"This case is especially interesting because it's one of the few search engine optimisation attacks that we have seen targeting a single, specific brand."

According to the Anti-Phishing Working Group, scareware packages have been rising in recent months as crooks turn to their use and now number more than 9,000.

BBC's Botnet Attack.

The BBC's Click program recently purchased a spam email program via the Internet to carry out an experiment to see how easy it was to become a spammer.

With the software available it turns out it is not difficult at all.

For those who don't know, a botnet is a collection of (usually) home PC's that are poorly protected and used by criminals to send spam emails.

It's not unusual for the owner of the PC to be completely oblivious of the number of spam emails sent from their machine. Sometimes the only indication is the fact that the PC is running slowly when connected to the Internet.

More information and to view the program at:

http://news.bbc.co.uk/1/hi/programmes/click_online/7932816.stm

Youngsters warned of social networks' threats

The UK's national internet security awareness campaign has warned that young people are leaving themselves wide open to exposure to online threats due to the way they conduct themselves online.

www.GetSafeOnline.org has warned that youngsters, especially students, are often in the dark about how they could cause internet security nightmares for themselves by sharing sensitive details.

According to Tony Neate, the campaign's managing director, the sensitive information left on social networking websites could be used to conduct online fraud.

"Students are on the internet all the time...but they don't necessarily know what the security implications are of that and they give away information," he explained

"People automatically think they've got to fill every box in," he said of the requirements of joining most of the sites, adding that they should not give out their date of birth.

"That's giving additional information that you don't want to give out," he advised.

Such sites include Facebook, MySpace, BeBo and Friends Reunited among others.

Amazon refuses to be tracked by Phorm

Online shopping giant Amazon has declared that it will not allow its website to be monitored by the targeted-advertising company Phorm.

Phorm monitors users' surfing in order to serve highly targeted advertisements. Its technology is currently being trialled under the name 'Webwise' by BT, with the users' consent. However, BT's first two Phorm trials, carried out in 2006 and 2007, did not have user consent, and last month, the UK government's failure to censure BT or Phorm for those secret trials resulted in legal proceedings against it by the European Commission.

In a brief statement last month, Amazon said: "We have contacted Webwise requesting that we opt-out for all of our domains."

Any owner of a website is free to opt out of having that site tracked by Phorm, and Amazon is the most prominent site operator to do so. Other services that recently opted out of the scheme include the blogging platform LiveJournal and the parenting community Netmums.

On 22 March, campaigners at the Open Rights Group (ORG) sent an open letter to seven companies, including Amazon, calling on them to opt out of Phorm's tracking. The organisation was not convinced that users would have enough information about Phorm's technology to give informed consent to being tracked, ORG chief executive Jim Killock said in the letter.

Killock said that content providers such as Amazon "need to know what the public feeling is and that their users are very concerned".

"We are glad that Amazon have [opted out] and taken the lead," Killock said on Wednesday. "They are the first household name to do this. We think it's right because what books you read is potentially sensitive [information]. We think it's particularly good in the light of the EU decision to bring action against the UK government."

Killock said he did not know Amazon's specific reasons for rejecting Phorm's tracking, saying that the company did not inform the ORG of its decision. However, Killock did say it was "important that other leading companies stand up for the rule of the law on the internet and block Phorm and make that publically known".

To date, none of the other six companies addressed by the ORG's letter — namely Microsoft, Google/YouTube, Facebook, AOL/Bebo, Yahoo and eBay — has made any statement on whether they intend to opt out of Phorm's tracking.

A spokeswoman for Phorm said on Wednesday that it was the company's policy to not comment on specific cases of publishers opting out of the tracking system.

Spotify, An Alternative to Music Piracy

The music industry has taken some extreme measures to counter piracy, but it hasn't found the silver bullet yet. The key is to come up with a service that will fulfil the needs of music lovers, and one that would even be embraced by the most hardcore pirate. With Spotify, this might just become possible.



Spotify is a music service that gives users access to a huge library of music, through a lightweight application that looks like a cross between the best parts of iTunes and Last.fm.

Music is streamed, partly supported by P2P technology, but it plays instantly, like we've never seen before.

One of the software engineers at Spotify is Ludvig Strigeus, the creator of uTorrent. It is therefore no surprise that the application uses very few resources, just 12k memory when we tested it. The rumour goes that some of the money made when uTorrent sold to BitTorrent Inc., has actually been invested in Spotify, an application that competes with piracy.

When we asked Andres Sehr of Spotify to describe the service, he told us "Spotify is a new way of enjoying music. We believe Spotify provides a viable alternative to music piracy. We think the way forward is to create a service better than piracy, thereby converting users into a legal, sustainable alternative which also enriches the total music experience."

The quality of the music on Spotify is comparable to 160kbps MP3s, which is more than decent for a streaming application. To fill its library, Spotify has made deals with EMI, Warner Music, Sony BMG and three other major labels, which all responded positively to the new concept. Interestingly, Spotify also uses P2P technology to stream the more frequently accessed tracks.

"Spotify uses a hybrid p2p system where music is delivered both by our servers and using P2P," Andres Sehr said. "This allows us to deliver the long tail of music which may not be very popular, as well as quickly serve up the latest hits that the majority of users listen to. P2P allows us to both increase the speed that we deliver music and also lower the cost of streaming it."

Aside from being a music streaming application, Spotify also allows users to create and share playlists with each other, the top 100 tracks of 2008 according to Pitchfork editors for example. On top of that, the Spotify interface helps you to discover new artists with its "similar

artists" and "artist radio" feature.

The overall response from Spotify users seems to be very positive, but can it compete with piracy? Time will have to tell, but Spotify invites are actively being traded within the BitTorrent community, and it has even been well received on some of the most elite music trackers.

One user at the music tracker What.cd wrote: "Honestly it's going to be huge. I've been browsing and playing from its seemingly endless music catalogue all afternoon, it loads as if it's playing from local files, so fast, so easy. If it's this great in such early beta stages then I can't imagine where its going. I feel like buying another laptop to have permanently rigged."

Spotify is not perfect though. One of the mentioned downsides is that it is not compatible with iPods and other portable MP3 players. The Spotify team hasn't ruled out the option of an iPod compatible version in the future, but for now they will focus on optimizing the Windows and Mac application.

Overall we can conclude that Spotify definitely has potential, but time will tell if it's able to compete successfully with piracy.

Spotify is currently in Beta stage, the free (ad-supported) version can only be used in the UK, Sweden, Finland, Norway, Spain and France.

Holes discovered in Trend Micro security apps

Nikita Tarakanov of Russian-based security company Positive Technologies reports several privilege-escalation vulnerabilities in Trend Micro Internet Security 2008 and 2009, including the Pro versions. The problems stem from improper data validation, which could allow a local user to gain excessive privileges on the system.

As far as I know, there's no fix available from Trend Micro, even though the problem was initially reported to the company on Feb. 4 and again on Feb. 12.

Positive Technologies didn't receive a response from Trend Micro, and on March 31, a third party disclosed details about the problem, according to Positive Technologies. The security firm then went public with its information about the weakness.

As you might expect, a working exploit of this hole is now circulating, so Trend Micro needs to address the problem quickly. Until patched versions of the programs are released, there's nothing you can do to protect your systems from the exploit.

Microsoft extends Red-Ring-of-Death cover to fresh Xbox fault

Just as Microsoft had recovered from the Xbox 360's notorious "Red Ring of Death" (RRoD) fiasco another big hardware error has begun slaughtering its boxes.



The Xbox 360 "E74 error" has become enough of a problem that Microsoft is now covering it under the console's extended three-year warranty reserved for RRoD failures. Redmond is also retroactively covering the issue, reimbursing customers who've already paid for E74-related repairs.

Gaming sites that have been tracking the error, most notably Joystiq,

<http://www.joystiq.com/2009/03/23/more-survey-data-backs-up-xbox-360s-e74-increase/>

indicate the E74 error has become increasingly frequent since mid-2008. It's believed most E74-related issues are caused by solder on the Xbox 360's ANA/HANA scaling chip coming loose rather than the RRoD's CPU/GPU problem.

Before the error, the console usually displays graphical glitches such as lines across the screen or static. The box's final death rattle comes as the on-screen E74 error message informing the user in several languages to contact Xbox customer support. There's also typically a single red light lit up at the lower right quadrant on the "ring of light" on the front of the console.

Standard warranty for the Xbox 360 is one year, but Microsoft had extended the warranty for RRoD failures to three years after the error proved a source of an "unacceptable number of repairs." Until recently, E74 was only covered by the Xbox 360's normal warranty - so E74 victims footed the repair bill after the year was up.

Microsoft is now including E74 failures in its extended three-year warranty. Customers who already paid for E74-related repairs will also automatically receive a refund within four to 12 weeks, the company said today.

From Microsoft's E74 support page:

While the majority of Xbox 360 owners continue to have a great experience with their console, we are aware that a very small percentage of our customers have reported receiving an error that displays "E74" on

their screen. After investigating the issue, we have determined that the E74 error message can indicate the general hardware failure that is associated with three flashing red lights error on the console. As a result, we have decided to cover repairs related to the E74 error message under our three-year warranty program for certain general hardware failures that was announced in July 2007. We have already made improvements to the console that will reduce the likelihood of an occurrence of this issue.

Hopefully, Microsoft learns its lesson here and will spend a little more on parts in the future to save millions of dollars in repairs.

Oddly, these hardware failures haven't turned into a PR nightmare for the company. The Xbox 360s shoddy insides have received a fair share of flack from the press, but the console still sells extremely well - certainly better than Sony's PS3 which, by most accounts, runs as solid as a rock (albeit an enormous and expensive one)

Relocate Vista's Documents folder

"Ask the Doctor"

"My Vista install really works great. I'd like to clean up some of the mess made when I transferred files from my old XP machine to the new computer, which came with Vista Business.

"One issue is how to get the Documents folder to reside on a second, roomier 1TB hard drive. It was easy in XP, but not so with Vista."

You have probably seen instructions that involve editing the Registry to change Vista's default folder. Both XP and Vista offer a much, much easier way to make the change.

To change the location of Vista's Documents folder, right-click the folder and select Properties. Choose the Location tab and click Move. Navigate to and select your preferred location for your Documents folder. Windows will ask if you want to move everything in the current folder to the new one; you probably want to say yes.

(The steps are similar in XP: right-click the folder, choose Properties, and click the Target tab. In most cases, you'll find the same Restore Default, Move, and Find Target buttons as in Vista's dialog box. If you see only a text box under "Target folder location," enter the new location for the folder there and click OK.)

Windows will then make the move for you, placing your Documents folder and all its contents in the spot you chose. The same steps work for moving any Vista folder that shows a Locations tab when you right-click it and select Properties. It's as simple as that!

Important updates

Microsoft anti-malware tool fixes Facebook bugs

An interesting addition to last month's update to Microsoft's Malicious Software Removal Tool (MSRT) was the ability to detect a virus that entered systems from the Facebook social-network site. Messages enticing Facebook users to watch a video would instead launch the Koobface virus.

Microsoft and Facebook worked together to add Koobface detection to MSRT, as discussed by Jeff Williams in the Facebook blog.

<http://blog.facebook.com/blog.php?post=68886667130>

Several people who install the MSRT update each month as part of Windows update ask us, "Does this program really do anything?"

The fact that you never see MSRT in action is actually a good thing; if you don't see any malware alerts, your PC probably isn't infected. In this case, silence is indeed golden.

Computer Doctors FREE testing

As repairers we obviously like to get paid for the work that we do. But we also like to give a bit back to our local community. That's why we have various FREE tests that we and you can carry out to keep your PC in top health.

Workshop Hardware Test.

We usually run these overnight as the full test takes from 5 hours. It tests all the electronics of your PC without using Windows software.

Email Test.

Lots of people have problems with Emails. You can send an email to our test account and it will send one back to you. More comprehensive than sending one to yourself.

mail.computerdoctors@keme.co.uk or click the link at the very bottom of the page.

Broadband Speed Test.

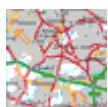
Check to see if your broadband is as fast as you think it is. Not all ISP's are the same!

<http://www.computerdoctors.uk.net/pages/bband.htm>

Computer Doctors Ltd
Unit 12 Blackthorn Ind.
Est.
Blackthorn Road
Northampton
NN3 8PT

If this has been passed to you from a friend and you would like your own regular copy, just go to:

www.computerdoctors.uk.net/pages/newsletter.htm



Map to our Northampton Workshop
www.computerdoctors.uk.net/pages/map.htm

Contact us

General information & to book a call out

Tel: 01604 411 444 (9-6 Mon-Fri, 9-1 sat)

Sales & On-Line Purchases

Tel: 01604 415 984 (9-6 Mon-Fri, 9-1 sat)

Fax: 0871 251 9099

Email: sales@computerdoctors.uk.net

Shop: www.computerdoctors.uk.net/shop

Technical Support

Free: tech@computerdoctors.uk.net

Tel: 0905 121 1097 (9.30-4.30 Mon-Fri)

(Calls cost £1.00 per minute)

Web: www.computerdoctors.uk.net

Email test Facility:

mail.computerdoctors@keme.co.uk

