Krebs on Security

In-depth security news and investigation

About the Author
About this Blog

Yep, There's a Patch for That

Digg

submit

Hello there! If you are new here, you might want to **subscribe to the RSS feed** for updates on this topic. You may also subscribe by email in the sidebar ➡ X

The average **Microsoft Windows** user has software from 22 vendors on her PC, and needs to install a new security update roughly every five days in order to use these programs safely, according to an insightful new study released this week.

The figures come from security research firm **Secunia**, which looked at data gathered from more than two million users of its free Personal Software Inspector tool. The PSI is designed to alert users about outdated and insecure software that may be running on their machines, and it is an excellent application that I have recommended on several occasions.

Stefan Frei, Secunia's research analyst director, said the company found that about 50 percent of PSI users have more than 66 programs of installed.

"Those programs come from more than 22 vendors, so as a first order estimate the number of different vendors you have on your box is the number of different update mechanisms you have to master," Frei said. "This is doomed to fail."

Secunia chief security officer **Thomas Kristensen** said his company is just a few months away from releasing a free, new tool that will automate the installation of software updates for dozens of commonly-installed third party programs. Kristensen said the tool will allow users to exclude certain applications, in the event that they don't want to automatically update specific programs.

Such an application, if done right, broadly adopted, and not resisted by third-party software vendors, could well reduce the number of Windows users whose machines get trashed by drive-by downloads, as all of these malicious or hacked sites try to silently install malware by targeting security holes in third-party software, such as **Flash** and **Adobe Reader**.

If I seem excited about the availability of a free meta-patching tool, it's probably partly for selfish reasons. Such a tool would almost certainly spell relief for anyone who is unlucky enough to be the appointed tech support guy for their family and friends, since fewer vulnerable applications means fewer compromised PCs, and hopefully less frequent pitiful pleas for help.

A copy of the Secunia study is available here (.pdf)

SHARE

Tags: patch madness, secunia, stefan frei, thomas kristensen

This entry was posted on Friday, March 5th, 2010 at 12:16 am and is filed under Time to Patch. You can follow any comments to this entry through the RSS 2.0 feed. You can leave a comment, or trackback from your own site.

61 comments

1. *Rick*
   March 5, 2010 at 1:47 am

   Hidden due to low comment rating. Click here to see.

   Poorly-rated. Like or Dislike: 👍 8 👎 32

Reply

2. *Dave M*
   March 5, 2010 at 3:03 am

   Hidden due to low comment rating. Click here to see.

   Poorly-rated. Like or Dislike: 👍 8 👎 33

   Reply

   - *Peter*
     March 5, 2010 at 3:32 am

     That's only part of the problem. The lack of tools for centralised management of installed software (such as the package management systems seen on UNIX-like operating systems) makes keeping your software up to date rather cumbersome. No wonder people don't keep up with such things.

     Well-loved. Like or Dislike: 👍 17 👎 1

     Reply

   - *ypwnme*
     March 5, 2010 at 7:05 am

     Dave,
     Have you heard about the concept of 'Defense-in-depth" ?

     Like or Dislike: 👍 2 👎 1

     Reply

     - *Patrick*
       March 8, 2010 at 7:25 am

       That's exactly spot on – Defense in Depth.

       There are just too many people out there who do not keep their software updated or do not know how to do so for reasons of:
       == No time
       == Lack of skills/capability
       == Scared of updating their PC
       == The person thinks they are so super-advanced that they know what they're doing when they really don't or
       == The PC is too old to keep reliably updated

       This nonsense about moving away from Windows to other OSs to resolve the issue is, well, you've all read the various low rated comments I'm sure.

       Like or Dislike: 👍 0 👎 2

       Reply

3. *Sean*
   March 5, 2010 at 6:24 am

   Alternate headline: Microsoft & The Security Cottage Industry announces an idea that is entirely unoriginal.

   Linux and FreeBSD have a (gasp) package management system with security plugins that can track vulnerabilities and advise updates.

   http://magazine.redhat.com/2008/01/16/tips-and-tricks-yum-security/

   http://www.freebsd.org/doc/handbook/security-portaudit.html

   Hot debate. What do you think? 👍 16 👎 18

   Reply

4. *ypwnme*
   March 5, 2010 at 7:05 am

   To Dave M:
   Have you heard about the concept of 'Defense-in-depth" ?

   Like or Dislike: 👍 1 👎 0

Reply

5. *Tudi*
   March 5, 2010 at 7:09 am

   I think this software will fail in 80% of the cases at least. I still use old winamp, old text editor and a lot of old versions. Sadly companies do not patch old versions but add new features, bugs and complexity that most people simply do not need.
   The idea is nice, but i still think that a proper solution is to stop the issue from the source instead of multiple patches (if possible)

   Hot debate. What do you think? 👍 12 👎 11

   Reply

   - *xAdmin*
     March 5, 2010 at 11:06 am

     Great point of newer software adding complexity and bugs. That's one reason I'm sticking with Windows XP versus Windows 7. That and the sticking new Taskbar design! Ugh. ☹

     Thankfully, XP will still get security updates through April of 2014! 😀

     Like or Dislike: 👍 2 👎 5

     Reply

     - *xAdmin*
       March 5, 2010 at 11:11 am

       Oops. Meant, "stinking new taskbar design" ;P

       Microsoft Support Lifecycle for Windows XP
       http://support.microsoft.com/lifecycle/?C2=1173

       Like or Dislike: 👍 1 👎 0

       Reply

   - *Stan Stahl*
     March 5, 2010 at 7:25 pm

     Writing software without bugs has been the holy grail of the software engineering profession for more than 30 years. While much has been done — both in theory and best practices — the best one can expect is to lower the bug count, not eliminate it. The problem is exacerbated by the hordes of application and web site developers with little or no training in writing secure code. We can't rely on the false promise of error-free code but must continue to apply defense-in-depth strategies to make up for imperfections in software [as well as imperfections in users and processes].

     Well-loved. Like or Dislike: 👍 6 👎 0

     Reply

6. *wahnula*
   March 5, 2010 at 8:06 am

   I have lots of legacy programs like Tudi, but the older and less-used a program is means that there will be less effort spent trying to compromise it, so I see that as a minor problem.

   The malware writers target the most-used programs for the best ROI, thus not all of those 22 vendors will be targets. We all know the current crop of characters behaving badly, I see nothing wrong with (and welcome) a FREE program that will check for updates to your PC's most-targeted apps.

   Well-loved. Like or Dislike: 👍 10 👎 0

   Reply

7. *AlphaCentauri*
   March 5, 2010 at 8:33 am

   It's a great idea if it doesn't start installing unwanted toolbars on my browsers after a couple years, like all the other great free apps seem to start doing.

   Well-loved. Like or Dislike: 👍 20 👎 1

   Reply

8. *Matthew*
   March 5, 2010 at 8:42 am

   If you’re not patching all your apps (Hi, Dave!) why bother patching Windows? Unless all attack vectors are blocked you are going to get bit.

   Like or Dislike: 👍 1 👎 1

   Reply
9. *xAdmin*
   March 5, 2010 at 8:43 am

   As some have already pointed out, Defense in Depth. Part of which these days involves LIMITING the software you install on a computer to not only reduce the amount of patching needed, but to reduce the attack surface of the system.

   As an example, my personal systems:
   Base install of Windows XP SP3 (running as limited user)
   IE8 (no added toolbars or add-ins besides Flash Player)
   Windows Media Player
   Flash Player
   MS Office 2003 with only programs I actually need (Outlook, Word and Excel) and of course the latest Office service pack
   Foxit Reader
   Roxio Easy CD Creator (base install of only CD Creator and CD Copier)
   Symantec Antivirus
   MVPS blocking hosts file (updated at least monthly)

   That’s IT! Easy to maintain/patch manually. Low attack surface. No worry that something is out of date/unpatched.

   Your mileage may vary, but the point is, if you limit the software installed, you reduce complexity and make it easier to secure and maintain your system.

   Well-loved. Like or Dislike: 👍 8 👎 3

   Reply
   - *Lofti*
     March 5, 2010 at 5:45 pm

     I’m sure your system works (except for the IE part, wouldn’t you be safer with Firefox?) but it would take about 80% of the fun out of having a computer for me. Why limit yourself that way?

     Like or Dislike: 👍 3 👎 0

     Reply
     - *JCitizen*
       March 5, 2010 at 6:05 pm

       FireFox has a serious security flaw, last I checked and there was no solution as of yet. Correct me if I’m wrong.
       If he is using Vista/Win7 xy64 he doesn’t have as serious a security problem as the venerable FF.

       Don’t get me wrong, I use FF, in fact I’m using it right now; but I have a lot of in-depth defensive apps on this install, so I’m not as worried as he may be.

       Like or Dislike: 👍 1 👎 5

       Reply
       - *John B*
         March 5, 2010 at 6:41 pm

         If you are talking about the flaw that the PSI software flags, look at the forum comments about that from PSI. There seems to be some legitimate doubt as to whether there really is a vulnerability.

         Like or Dislike: 👍 0 👎 0

         Reply
         - *JCitizen*
           March 5, 2010 at 10:20 pm

           I did follow all links and information on the subject, and Secunia is standing fast on their assessment.

This company is wholly dependent on reputation, and has been found to be correct in all reports so far, including open source vulnerabilities. If they let that fall by the wayside, they wouldn't be in business long, and I'd be the first to drop them.

It is no secret that Google has been cutting back support for the Mozilla foundation, and concentrating on their own browser. Discussions everywhere are speculating that developers are finding it hard to keep up, and Chrome developers really don't want the competition.

I can't use Chrome, so don't just assume I'm a shill; I tried their browser, but it wouldn't open on 64 bit systems in the standard account mode, so although it might make a good administrative browser, I can't really see having three browsers.

As soon as I get the money, I am going to donate to the Mozilla Foundation, and some of their add-on vendors too! I suggest everyone consider this option.

Like or Dislike: 👍 3 👎 1

10. *Ben Moore*
    March 5, 2010 at 8:47 am

    Isn't it ironic that a security company (Secunia) publishes a document on security exposures in a format (.pdf) that has such a reputation of security exposures that Brian has to annotate that it is in a risky format?

    Well-loved. Like or Dislike: 👍 15 👎 10

    Reply

    - *GiddyUpGo*
      March 5, 2010 at 9:19 am

      Yes…also Secunia requires that you have Adobe flash installed, another very insecure program that is always having problems. I have not had adobe flash installed for years. The sites that require it can do their thing. I simply move on to another site and never miss them!

      Hot debate. What do you think? 👍 3 👎 6

      Reply

      - *JCitizen*
        March 5, 2010 at 10:26 pm

        The personal software inspector works under Vista without the Adobe add-on. It just doesn't show the charts and graphs with out it. I've used it without it, and it still seems to work.

        At least you can get the notifications of what is insecure,end of life, and needs updating. You just may not be able to click the download button to do it from the GUI.

        Like or Dislike: 👍 3 👎 0

        Reply

11. *Mike F*
    March 5, 2010 at 8:59 am

    I have been patching systems with Secunia for awhile, and I find it has been very useful in finding some of the vulnerabilities that are on users systems. Whenever someone brings me a computer I run the online app to see what software needs to be patched. A free application that would automatically update would be even better, and like you Brian, I got excited when I heard this. Hats off to Secunia for offering something like this to help the overall security environment. I doubt very seriously that they are going to be implementing foolish toolbars or the like, but anythings possible.

    Well-loved. Like or Dislike: 👍 11 👎 0

    Reply

12. *Michael Horowitz*
    March 5, 2010 at 1:43 pm

    Good for Secunia! Windows users need something like this in the worst way. Unpatched software is a huge problem that doesn't get the mind share it deserves.

    I'm a big fan of Secunia's online software inspector. Even though it does not test as many applications as their Windows app, it's hard enough to get a clean bill of health.

    http://www.esecurityplanet.com/article.php/3847091/Check-All-Your-Windows-Patches-Secunia.htm

One thing to be on the lookout for when this application is released: Does it flag software with known bugs for which there is not yet a fix? This is the one problem with their online application, it fails to flag these cases.

Like or Dislike: 👍 3 👎 0

Reply

13. *John B*
    March 5, 2010 at 2:06 pm

    Thanks for the post on the Secunia software. I had not heard of it before. I ran it on all 3 of my PCs at home. While it did not identify any unpatched software (I keep up with that) it did alert me to several old versions on my machine that I no longer needed and could safely delete.

    One reason that I follow your blog is to keep up with issues that need action on my PCs (I am the family tech support…). A good addition to your blog would be a post that summarizes the recommendations for how to keep your PC secure. I’m thinking of recommendations for sound antivirus programs, scanners (e.g., superantispyware) , browsers, settings (such as turning off javascript in Adobe reader), etc. There is no need to pick one best package, just those that are solid choices. These tips are all over your blog but could be usefully summarized and kept reasonably current in one place.

    Well-loved. Like or Dislike: 👍 6 👎 0

    Reply

    - *JCitizen*
      March 5, 2010 at 5:42 pm

      Here’s my list – maybe Brian will follow up someday. But I think he would like to avoid looking like a shill, so I have my doubts:

      Snoopfree Privacy Shield
      Comodo Firewall Pro
      AdAware Free
      Spybot Search & Destroy
      Malwarebytes anti-malware
      Avast or[NOD32 if you have money]
      Spyware Blaster(Javacools)
      MVPS host file, or AdBlock Plus
      Secunia PSI
      CCleaner and/or Revo Uninstaller
      GMER rootkit detector
      LastPass – password and personal data vault

      I have an even larger short description of each if you really are interested.

      I do not work for any company or person, I just hate malware to pieces!!

      Like or Dislike: 👍 2 👎 2

      Reply

      - *John B*
        March 5, 2010 at 6:38 pm

        Many of the products that you list are new to me. I would be interested in the short descriptions that you mention. How can I get to them?

        Like or Dislike: 👍 0 👎 1

        Reply

        - *JCitizen*
          March 6, 2010 at 12:12 am

          Okay,

          Here is my recommended list, bear in mind I lean toward free, I’ve found they almost always work better(sometimes the paid version doesn’t):

          1. SpywareBlaster – for those that refuse to use NoSript. Protects against bad Active X files. Host
          files also helps protect against bad servers that inject malware thru previously legit web-pages.
          AdBlock Plus a must for FireFox too, on top of SB’s active x protection.

          2. A good malware scanner like MalwareBytes,anti-malware, AdAware, A-squared, or SuperAnti-spyware. MBAM’s real time protection is worth paying $24 for lifetime license.

3. Comodo Verification Engine – helps identify sites with poor SSL encryption or other problems, including phishing or bad practice on certification. I use Networking4All.com to find out just what in Secure Socket Layer server setup, is wrong with the site, that is pegged insufficient or insecure.

4. Password vault – to protect passwords, credit card numbers, personal ID, etc. LastPass is free and keeps your information off the computer, and encrypted in the cloud, through SSL communication. Comodo has a free one called iVault.

5. For XP got to have SnoopFree Privacy Shield – A fantastic I/O firewall to keep unknown keyloggers
and spys from seeing your video image login snapshots – may not protect fully against kernel mode rootkit spys. For Vista/Win7 Prevx claims the same thing for a fee, but if your a facebook subscriber they are giving it away free for now. Prevx is supposed to block ALL screen, and keyboard spys.

Spyware doesn’t have to necessarily install to get this information. Or if there isn’t a definition out yet, they can do a lot of damage in the mean time. Some of the new threats are reportedly cross platform capable, so nobody is necessarily safe, esp. from root kits; some of which can remain resident during reboot and install their own kernel.

6. Identity Finder can help mitigate this, as a criminal cracker doesn’t necessarily need to read your inputs, (s)he can get it from the hard drive if you don’t use a password vault. Its a good idea to run ID Finder on your hard drive after installing a password vault to remove any social security numbers, credit cards or saved passwords that may be left behind. You must uninstall after use; a good ROM USB would be a good way to use it. We don’t want to make the cracker’s job easy and leave any code left behind that he can use against you.
(Update) The new one is supposedly password protected – use your own judgment.

7. CCleaner and Revo uninstaller – either of which can surprise you when you find out what kind of crap is actually installed without your permission or knowledge. CCleaner can help mitigate some of the malware that may be resident in the hidden temp files, but it can’t get them all. This is the SAFEST registry cleaner I’ve EVER used!!

8. Site Advisor – it may be three months behind in site evaluations, but it is better than nothing. NIS 2009 has a better paid one(Symantec) – FireFox has a better free one as a plug-in – Link Extend is the best rated by experts world over. WOT – is tried and true.

Symantec was a total failure until NIS 2009, but I have clients running NIS 2010 on older P4 processors that work just fine.

9. Rootkit detector – Ice Sword is best if you can trust the Chinese originator of this ingenious root kit detector; I use GMER, not so much that I trust the author, but it has a good track record that is trustworthy. Most clients like BlackLight. you have to drill down on the F-Secure site to find the free one. DarkSpy has a rep – I’d check the CNET user reviews on that one. Most technicians agree using all four is best, as some only detect, and others remove(if your careful). Ice Sword must be pre-installed to get a system snapshot.

10. Comodo with only the firewall enabled, Defense+, which was part of it, will no longer work with Snoopfree Privacy Shield installed. I have not yet found a work around. Comodo may have an update by now. Defense Plus is one of the best HIPS defenses ever made. It works fine on Vista with everything on this list including Prevx.

Also – I always make sure Comodo firewall is on DSL clients and SMBs that have more than one computer on their LAN. Even the new Windows firewall has been compromised on some of my clients networks. Including my sister. I feel Comodo is more leak proof for folks who aren’t that whippy at configuring firewall rules. Consider getting any good hardware firewall recommended on Tom’s hardware. I like ZoneAlarm’s Z100 – I DO NOT like ZoneLabs software firewall. It has been an unmitigated disaster on my honeypot.

11. Avast – still the only free anti-virus worth having on the PC at all. I have yet to see it loose a battle on a PC with in depth defenses. I rarely have to scan with it, as it always reacts as soon as the virus tries to establish itself on the machine. Avast relies on one of the best heuristic engines ever devised, and doesn’t necessarily always need to be full up to date to work. I’ve witnessed this in the lab, if you not sure, just quarantine it, and Avast will usually know within a week if it is dangerous or not.

The new malware seem to be aware of what type of defense you have, and may lie dormant in temp files waiting for a vulnerability. I have NEVER been let down by Avast. Sometimes, while double checking using and online scanner or Prevx, it will suddenly come to life when it senses the malware trying to evade the other scanner, and WHAM!! It is all over for the malware! I’ve never found malware by scanning with Avast, except upon installation – the battles I’ve seen can be very interesting – so I don’t worry about it. Just for performance check, I may run it every quarter, but that is it.

GDATA is not free, but very economical, and they say it uses a combination of Alwil’s heuristic engine, with Bit Defenders scanner. My clients have had very good experience with it, and it was THE top rated AV in the late 2009 AV comparatives tests. I could not get the Vista x64 version to install correctly, your mileage may vary.

12. Last but not least is Secunia PSI – this helps the client patch the myriad of applications that can leave even a good secure operating system wide open. Patching applications can almost make anti-malware obsolete if you run regularly as a restricted user on a Windows; I use it concurrently with File Hippo’s update checker.

Well-loved. Like or Dislike: 👍 7 👎 1

Reply

- *John B*
  March 6, 2010 at 9:37 am

Thanks for posting! That list is very helpful. It still would be great if Brian created a post that summarized his recommendations. There is no need to be a “shill” for a product as its fine to recommend several products in each category if each is solid. A good example of what I am thinking of is Walt Mossberg’s annual buying guide for configuring PCs. Here is his most recent article from 2009.(http://ptech.allthingsd.com/20091028/operating-systems-offer-new-choices-in-pc-shopping/) I think there is a need for a similar type of article that addressed PC security products and best practices.

Like or Dislike: 👍 2 👎 2

14. *Jeremy G.*
    March 5, 2010 at 2:44 pm

    The idea of a one-stop patch manager for Windows is great. Unfortunately, no one who isn’t already motivated to keep up with patching is likely to go out of their way to install another stand-alone program. It’s only going to serve users who already understand the need for patching anyways…

    Like or Dislike: 👍 1 👎 0

    Reply

    ◦ *Mike F*
      March 5, 2010 at 10:42 pm

      I agree with you, however, if it is able to automatically update, it means more software patches will be applied to PC’s that normally would not get patched on a regular basis. If it is effective technicians will install it for more people and they won’t have to keep visiting those machines so frequently.

      Like or Dislike: 👍 0 👎 0

      Reply

15. *JCitizen*
    March 5, 2010 at 5:56 pm

    I like Secunia PSI and recommend it to all my clients, especially if they do any shopping/banking on line.

    I can’t wait to try the new version!

    One of the things I really like about using Secunia is that it usually doesn’t connect you to all the junkware vendors try to foist on you; just the file you need and no more. For the very few exceptions, I can simply put them on the block list.

    Also I don’t have to deal with arcane sites like Adobe and Sun Micro-systems, where it is a real pain to navigate for what you need. Secunia usually beats the regular java updater, which gives you a big jump on zero day exploits. File hippo update checker, sometimes beats Secunia PSI, so I use both of them!

    Keeping all applications updated has left many a malware clueless on my lab honeypot, as the malware cannot take advantage of known exploits to take over my installation. They may get as far as attempting to open the application, and then that is all. Usually I only need CCleaner to get rid of them, as they just sit there without a mission in the temp directories.

    Like or Dislike: 👍 1 👎 0

    Reply

16. *Gannon*
    March 5, 2010 at 6:23 pm

    I have a dual boot laptop, Ubuntu/Vista with a Verizon CDMA USB. The internet connection came with Windows software and has a usage limit after which I pay extra. I can only check the usage from Vista. Even the Windows automatic updates are a problem for me, since due to the usage limits I pay today for what I’ll get “free” tomorrow.

    And so my question, does the Secunia software allow you to add Microsoft itself to the list ? And, will they handle update downloads like Ubuntu (Canonical) and Microsoft (manual updates) ? That is give you a list and check boxes.

    Like or Dislike: 👍 0 👎 1

    Reply

17. *JBV*
    March 6, 2010 at 2:32 am

    If that “free meta-patching tool” had been installed and automatically patched Windows last month, then how many more BSODs would there have been?

The automatic updates on my computer are all turned off. (Except for AVG, which lets you disable its data base auto-updates, but not the program updates. Very annoying.)
Auto-updates interfere with programs that are running and download who-knows-what things without asking if you want them.

It takes self-discipline, and a lot of checking and monitoring, e.g., running virus programs updates every day, following Brian's recommendations, and regularly running Secunia, but I prefer to wait and see, rather than to have some unkown third party decide what to put into my computer (like tool bars that are downloaded with updates if not unchecked).

Like or Dislike: 👍 0 👎 0

Reply

18. *jona*
March 6, 2010 at 6:20 am

For regular home users, the Filehippo update checker goes a long way towards keeping the most common home use applications up to date very easily http://www.filehippo.com/updatechecker/

Like or Dislike: 👍 2 👎 0

Reply

- *JCitizen*
March 6, 2010 at 11:53 am

To John B., Jona and other readers who are interested.

If the plethora of security solutions has you befuddled and confused, and I don't blame you, by-the-way; please read the USER reviews at CNET for any software you may run across. They are very helpful and also indicate how long the solution has been established. I read the editor reviews but I find they don't always keep the special purposes that users need in mind. Balancing between the two sources is a wise decision.

Bear in mind the users are mostly amateurs, and therefor their judgment may be colored by prejudice; however, if you read between the lines, with that in mind, you will find them absolutely priceless in evaluating new or established software utilities.

Tom's hardware is an industry wide accepted source for finding good security hardware as well.

I hope these posts can help someone with their IT security needs; and help build a defense against the onslaught of criminal crackers who are out to rob us blind 24/7/365 days of the year!

Jona is right, File Hippo update checker can help you get the zero day jump on possible exploits out there on the web. It sometimes trumps Secunia PSI on getting there with the updates first, and even suggests betas that may solve future problems. The downloads are more reliable from them, than many sources, and can happen very fast!

It is also a good way to skip tripping through the minefields of junk add-ons for your updates, so it is well worth having!

Like or Dislike: 👍 0 👎 0

Reply

19. *JohnJ*
March 6, 2010 at 11:51 am

I find it strange that Adobe Reader Updater also updates Photoshop, but it doesn't cover Flash.

Like or Dislike: 👍 1 👎 0

Reply

- *JCitizen*
March 6, 2010 at 12:02 pm

Most IT technicians including myself, and those I discuss with, are pretty disgusted with Adobe, period. We are looking for alternatives at every juncture. Right now, if you have XP, there is a flash alternative called Gnash, I believe, which if you are good at open source installation, is supposed to work famously as a substitute.

I use Foxit Reader as a substitute for Adobe Reader. Amazon.com has many photo and video softwares that rate way higher than Adobe Photoshop. I say that at the risk of being flamed by Adobe fans, but I am sick and tired of Adobe's dereliction of duty in making secure software in the first place, and then halfheartedly providing patches when things go south.

Like or Dislike: 👍 3 👎 0

Reply

20. *Troy*

March 6, 2010 at 1:20 pm

Yes been using Secunia for about 6 months now.

Sandboxie is the program that can REALLY protect you from rogue software, spyware and malware.

1. Sandboxie http://www.sandboxie.com/

2. Microsoft Security Essentials

3. Malwarebytes Anti-Malware

4. Secunia

Like or Dislike: 👍 3 👎 0

Reply

21. *JCitizen*
March 6, 2010 at 2:17 pm

Sandboxie is a good tool, especially for XP users; however please be aware that their are VM aware malware out there that know how to take advantage of leaks in many VMs(virtual machines).

Many technicians tell me the standard account on NT6 machines is probably as good if not better. However using Chrome or Sandboxie on the Administrator account is wise advice.

I understand Chrome has a sandbox also.

Like or Dislike: 👍 1 👎 0

Reply

◦ *Troy*
March 6, 2010 at 3:01 pm

Yes I also use Chrome sometimes. Sandboxie and Chrome are compatible with each other. Working great together here. Sandboxie can also sandbox all the programs your running while you browse. such as Adobe Flash , Java , Foxit reader.

You can read on sandboxie's forum that there has been leaks but the author has patched those leaks within like 1 or 2 days. If you enable the start/run access option within sandboxie with drop rights there has been know known malware too bypass that.

Yes a Limited User Account in XP, Vista, 7 would be real secure also. Combine that with sandboxie and a good antivirus, with Secunia PSI and you would be near bulletproof.

Like or Dislike: 👍 1 👎 0

Reply

■ *JCitizen*
March 6, 2010 at 4:18 pm

True! We've heard from Sandboxie's developer over at Tech Republic; they seem like a pretty good team!

I tried Chrome, but it won't work on a x64 standard account yet. I haven't had a chance to try sandboxie, I've been eying some other VMs though.

Anybody tried Returnil? It has a lot of fans on download.com?!

I usually don't use my browser at all on the admin side, so I've been lazy about testing anything.

Microsoft's free Steady State is a good on for those of you tired of AV and AS maintenance. Better keep at least one of two of them whilst you are unlocking the drive for maintenance. After all, you would still want to update your operating system and applications, even if you freeze the OS.

Like or Dislike: 👍 1 👎 0

Reply

22. *Dewi Morgan*
March 7, 2010 at 9:14 pm

Anyone who uses "her" where "their" is more correct deserves a smack over the head with a good descriptivist dictionary. Unless the "average Microsoft Windows users" genuinely is female.

That said, the software looks like it might be very interesting: thanks for pointing it out!

Like or Dislike: 👍 0 👎 4

Reply

- *AlphaCentauri*
  March 7, 2010 at 10:56 pm

  "They/them/their" are increasingly being used as both singular and plural in casual conversation. I'm sure that as with "you," that usage will eventually become correct English grammar (and it won't be a minute too soon for me), but it isn't correct now. Don't give Brian a hard time for attempting to reflect the fact that computer users can be either male or female. There is no elegant way to do it in English at present.

  Like or Dislike: 👍 2 👎 0

  Reply

  - *lofti"*
    March 7, 2010 at 11:44 pm

    Correct! If using "she" or "he" is offensive then one is left with "he/she" or a variation there of. Using "their" instead of he or she when a singular pronoun is required bugs me.

    Like or Dislike: 👍 2 👎 1

    Reply

23. *JBV*
    March 7, 2010 at 9:46 pm

    Even a descriptive linguist would acknowledge that "her" is singular and "their" is plural. The pronoun refers to an "average Microsoft Windows user," also singular, of which I am one.

    That said, one can only wonder why you are posting here at all?

    Like or Dislike: 👍 1 👎 0

    Reply

24. *JCitizen*
    March 7, 2010 at 9:49 pm

    Well then! I guess we better get to smacking Thomas Kristensen, chief security analyst at Secunia, on the punkin' head! HA! 😀

    Like or Dislike: 👍 0 👎 0

    Reply

25. *Dewi Morgan*
    March 7, 2010 at 10:43 pm

    @JBV: "They" (like "you") has been singular as well as plural, from at least 1300 onwards. Merriam-webster.com cites such usage by Shakespeare, Austen, Auden, Thackeray and Shaw; other dictionaries also reference Swift, Shelley, Scott, and Dickens, as well as many other English and American writers. But if you don't like "they", and want to avoid "he", then "(s)he", "he/she", "he or she" are all widely used. "She" is just a bit barmy, is all.

    As for why I posted: I think it was quite clear. Even you seem to have understood it. Clearly, I posted to grumble (not to correct, just to grumble) about misuse of "she", and to thank for drawing my attention to a cool bit of software. For why I posted *here*: posting a reply to this post anywhere else would've been a tad strange, no?

    @JCitizen: How do you get that? This article claims Brian Krebs as the author. On the Thomas Kristensen blog: "to install the 75 patches from the 22 different vendors, he or she has to master more than 22 different updating mechanisms."

    Still, I didn't mean to derail discussion, and apologise for that.

    Back on topic, it's about ruddy time something like this came out for Windows, and tying in to WSUS is a nice move, too. It annoys me that every time I start a machine I've not touched in a couple of months, I need to update tons of software on it: done right, this may make it tons easier.

    Like or Dislike: 👍 1 👎 2

    Reply

- *lofti*
  March 7, 2010 at 11:54 pm

  We all know that Shakespeare made up all kinds of stuff 🙂 . Thanks for the history, every time I think I’m beginning to understand my native tongue I’m blindsided. Ain’t it great?

  Like or Dislike: 👍 2 👎 0

  Reply

26. *JCitizen*
    March 7, 2010 at 11:57 pm

    If you do a google for that exact phrase, you will find many references to Thomas as the source. I suspect some of them are simply typos or misquotes; but really are we so anal that we REALLY care!!?

    I’d say the subject at hand is more important, than a bunch of stuffy English teachers!

    Language is not a set thing, it is dynamic; who would have thought “Google” would be a verb, just a few years ago?

    Like or Dislike: 👍 0 👎 1

    Reply

    - *Dewi Morgan*
      March 8, 2010 at 12:48 am

      I stand corrected on the attribution, then. And no, I don’t care that much, and I’m feeling increasingly uncomfortable to have so derailed the topic. I shoulda known better, and I’m sorry.

      I completely agree that keeping our machines secure and up to date is the important thing here. I’m playing with the “OSI” on their site: just started it running, and I’m interested in what it finds.

      And yeah: I always thought it’d be “Yahooing”. Or even “Archieing”, back before the web.

      Like or Dislike: 👍 2 👎 1

      Reply

      - *JCitizen*
        March 8, 2010 at 11:11 pm

        Thank you for your participation here Dewi! I’m sure we all look forward to future discussions with you! We all love IT here! 🙂

        It is the nature of almost all IT people to be exacting in every detail, in which I’m sure you have the highest skills! If you are not in that venerable profession, you would be exceedingly proficient at it, by all my best estimates.

        Like or Dislike: 👍 1 👎 1

        Reply

        - *Dewi Morgan*
          March 9, 2010 at 12:14 am

          Thank you!

          I guess my codemonkey trade shows a tad. My current official job title as listed in credits is “Senior Monkey Button Pusher”: a jab at a previous job where we were all considered “junior monkey button pushers”.

          I was interested that there were differences between Secunia’s OSI, PSI and the Firefox plugin check at http://www.mozilla.com/en-US/plugincheck/ – I guess because one’s working off versions reported in Javascript, and one is looking at the exes. Or maybe one only lists security updates, and one only lists major point updates.

          OSI and Mozilla both found three outdated apps, PSI found four, but they all only agreed on one: Flash.

          Still not *hugely* impressed, though: I’ve got a good few hundred apps accreted over the years, I’d expect it to find more than four outdated. It’d also be nice to see which apps it’d detected, so I’d know which ones I’d need to check manually.

          Still cool though.

          Like or Dislike: 👍 1 👎 1

          Reply

- *Dewi Morgan*
  March 9, 2010 at 12:50 am

  Ah, the PSI has an "advanced" mode, which shows everything I wanted, and everything I didn't know I wanted, and also finds many more apps. Yay!

  Like or Dislike: 👍 1 👎 1

27. *JCitizen*
March 9, 2010 at 11:32 pm

In advanced mode you can also submit files you think should be added to their watch list, and they encourage it! There is really nothing quite like if for security professionals.

Like or Dislike: 👍 0 👎 0

Reply

Leave a comment

Name (required) □

Email (required) □

Website □

Comment □

Submit Comment

□ Notify me of followup comments via e-mail

- □
- FOLLOW ME ON twitter
-

SHARE

The Popular Ones...

- Would You Have Spotted the Fraud? (194)
- New Patches Cause BSoD for Some Windows XP Users (143)
- 'Time Bomb' May Have Destroyed 800 Norfolk City PCs (129)
- What Kind of Internet User Are You? (98)
- N.Y. Firm Faces Bankruptcy from $164,000 E-Banking Loss (95)
- Texas Bank Sues Customer Hit by $800,000 Cyber Heist (90)
- ATM Skimmers, Part II (83)
- Firm to Release Database & Web Server 0days (80)

Subscribe by email

Your email:
Enter email address...

Subscribe Unsubscribe

Recent Posts

- FBI: Online Fraud Costs Skyrocketed in 2009
- Crooks Crank Up Volume of E-Banking Attacks

- Secret Obsession: Odd Windows Crash Alerts
- Dozens of ZeuS Botnets Knocked Offline
- Microsoft Warns of Internet Explorer 0day

Categories

- A Little Sunshine
- Latest Warnings
- Other
- Target: Small Businesses
- The Coming Storm
- The Wire
- Time to Patch
- Web Fraud 2.0

Archives

- March 2010
- February 2010
- January 2010
- December 2009

Blogroll

- Arbor Networks Blog
- Bleeping Computer
- CERIAS / Spaf
- Cloudmark Blog
- Cyber Crime & Doing Time
- DHS Daily Report
- DSL Reports
- ESET Threat Blog
- F-Secure Blog
- FireEye Malware Intel Lab
- Google Online Security Blog
- Graham Cluley, Sophos
- Kaspersky Blog
- Knujon
- M86 Security
- McAfee Avert Labs
- Microsoft Malware Protection Center
- SANS Internet Storm Center
- Schneier on Security
- Security Focus
- Securosis
- StopBadware
- Sunbelt Blog
- Symantec Response Blog
- TaoSecurity
- ThreatExpert Blog
- TrendMicro Blog
- US CERT
- Websense
- Wired.com's Threat Level

Click it!

Donate

Tags

3fn ach fraud adobe adobe reader albert gonzalez atm skimmer atrivo bsod chinese dissidents 0day ehud tenenbaum estdomains esthost exploit pack fbi fdic firefox google idefense ie intercage internet explorer jotti kadima panamena mccolo microsoft moneygram money mules panda security rbn realplayer RSA russian business network sans internet storm center scansafe security fix blog small business victims twitter virustotal virustotla washington post western union windows wired.com zeus

Powered by WordPress. Theme design by BBID.