



Original URL: http://www.theregister.co.uk/2008/08/22/anatomy_of_a_hack/

Anatomy of a malware scam

The evil genius of XP Antivirus 2008

By [Jesper M. Johansson](#)

Posted in [Anti-Virus](#), 22nd August 2008 18:45 GMT

[Free whitepaper – Trend Micro enterprise security](#)

Anyone who has a blog has probably seen blog spam; comments to the blog that simply try to entice people to go to some other site. Most of the time the site being advertised is simply trying to boost its search engine rankings to generate more ad revenue.

The more links there are to a site, the more popular the search engines figure it is, and the higher up in the search results it ends up. Blog spam, therefore, is frequently thought to be a good way to boost the search engine rankings. In some cases this turns malicious. Some sites engage in wholesale intellectual property theft to [boost their rankings](#)

(<https://msinfluentials.com/blogs/jesper/archive/2007/12/20/idthieves-org-and-its-ilk-are-unauthorized-blog-mirrors-stealing-intellectual-property.aspx>).

A few of weeks ago, however, I started noticing something far more insidious. I moderate all comments

to my blog. This is something I started years ago to keep the blog somewhat family friendly, and to avoid propagating malicious content. Recently I also completely disabled trackbacks to avoid boosting the search engine rankings for sites that steal my work. This means I see every comment that comes into my blog. The other day I noticed one that contained nothing more than a link to a fake Google site: google-images.google-us.info/index.html.

This looked very suspicious to me so I made a note of it. Over the next several weeks I noticed a lot more of these, not only pointing to Google but also to Yahoo and MSN. The servers they pointed to all had the same basic structure, such as google-homepage.google-us.info, msn-us.info, yahoo-us.info, etc. Every one resolves to the same IP address: 124.217.253.8. That IP address is registered to Piradius.net in Singapore. The server appears to be hosted out of Kuala Lumpur. The domains, however, are registered in Ukraine:

```
Registrant Name: ermua
Registrant Organization: santa banta
Registrant Street1: lenina str. 43/67
Registrant City: Kiev
Registrant State/Province:
Registrant Postal Code: 0444
Registrant Country: RU
Registrant Phone: 044.763238
Registrant Email: yura_gpz@mail.ru
```

Domaintools.com confirms this. You will soon see a related domain, xpantivirus.com. That one is registered to Chebotarev Oleksandr, [in Odessa, Ukraine](http://whois.domaintools.com/xpantivirus.com) (<http://whois.domaintools.com/xpantivirus.com>). This had me very curious and I wanted to know more about what this site was attempting to achieve. Consequently, I fired up a virtual machine and started investigating. What I found was an interesting tale of trickery.

The First Hint

The first thing a potential victim would do is open up one of the sites. For my tests I used www.msn-us.info. I did my initial test on Windows Vista. After various trickery, I got the dialog in figure 1.

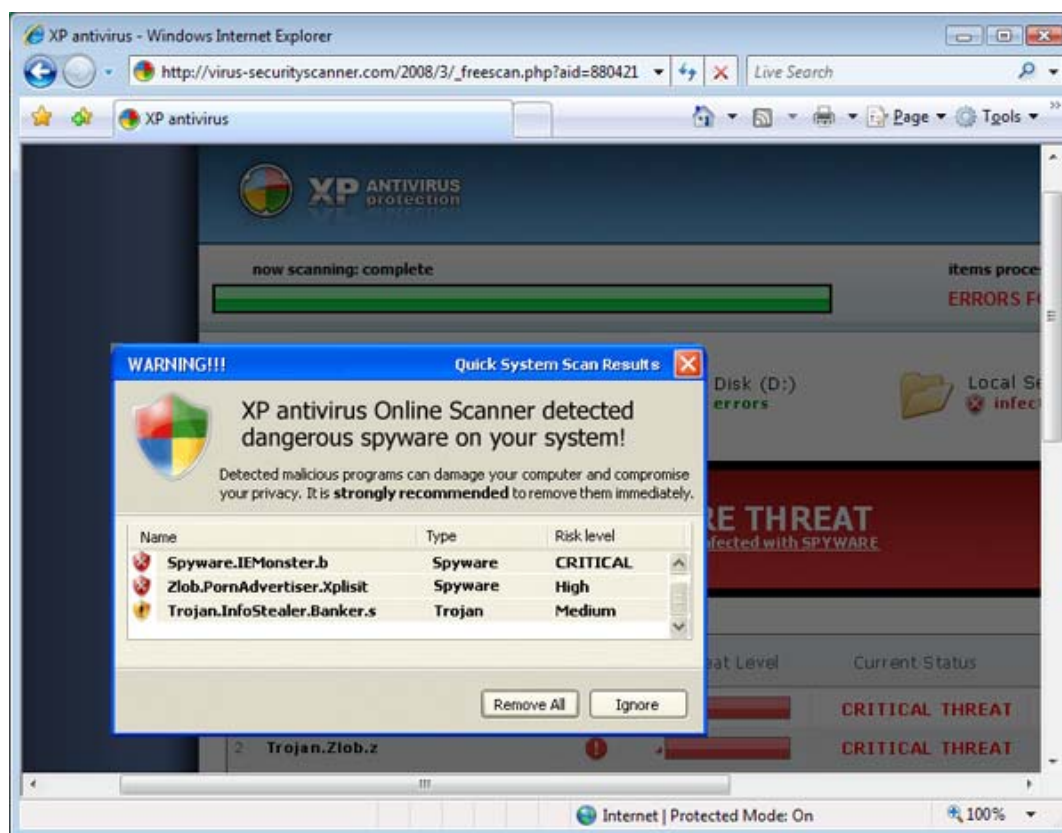


Figure 1 The site issues a redirect to a different site

Notice the chrome in Internet Explorer. My virtual machine is running Windows Vista. The popup, however, has the XP chrome. As it turns out, the popup is not a popup at all. The whole page is just one image, hyperlinked to a file download. I must give the criminals here credit for graying out the background to lend it credibility; a la Vista User Account Control (UAC). One of the questionable benefits of UAC is that it has conditioned people to believe that as long as the screen background is grayed out they can trust whatever is on the screen.

Before the popup in the screen shot there was actually another one too. That one was an animated GIF that looked like it was performing a virus scan of your computer. Needless to say, it found several pieces of fake malware on my computer, hence the dire warning in the fake popup.

If this looks suspicious to you, it should. We are not on www.msn-us.info. We are on virus-securityscanner.com. When you go to any of the sites that are linked in the blog comments you download a few files, and then it redirects you to <http://virus-securityscanner.com/2008/3/freescan.php?aid=880421>, where the last part is some form of identifier that we will return to shortly.

Similar sites to this one have been reported at least as far back as 2003. The modus operandi does not change, although the exact details of what the sites do seem to. It appears likely that these sites are all related and that there are multiple fronts for them. Virus-securityscanner.com appears to be hosted at an ISP in Pennsylvania at the time of this writing, but that is likely to change by the time you read this. In fact, between the time I started researching this and the time I wrote the article, the site name had changed to virus-onlinescanner.com.

Workflow Step By Step

At this point I was sufficiently curious to walk through the work-flow step by step. You may enjoy what I

discovered. Starting from the beginning, when I first went to www.msn-us.info I received the warning in Figure 2.

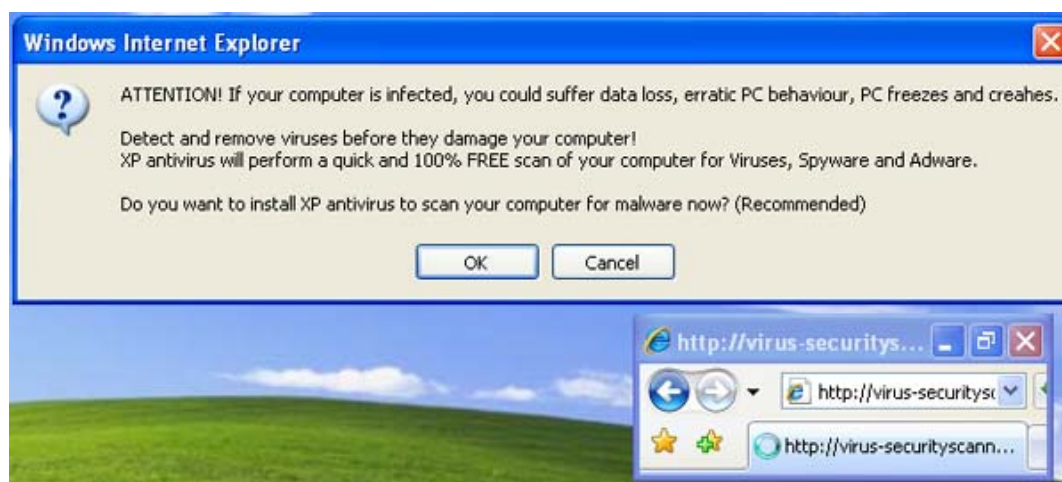


Figure 2 Initial warning

It is quite nice of them to warn me about malware. It's also nice that they are offering to solve all my problems for free. Note also that I repositioned the dialogs in Figure 2 so you can better see what is happening. Without doing that the very small web browser window is actually hidden behind the dialog to make it look as if the dialog is coming from your computer, not a web page. If you click "OK" in figure 2, you get figure 3. If you click cancel, it just goes directly to a download for a fake anti-malware program.

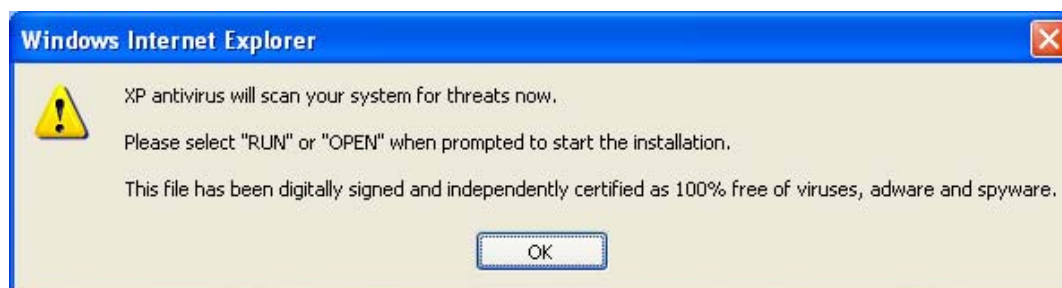


Figure 3 The malware is independently certified

The warning in figure 3 just lets you know that you are about to download something. Obviously the criminals are well aware that users are incredibly desensitized to warnings and the more warnings they get, the less they pay attention to them. Click OK in that warning, and you get the page in Figure 4.

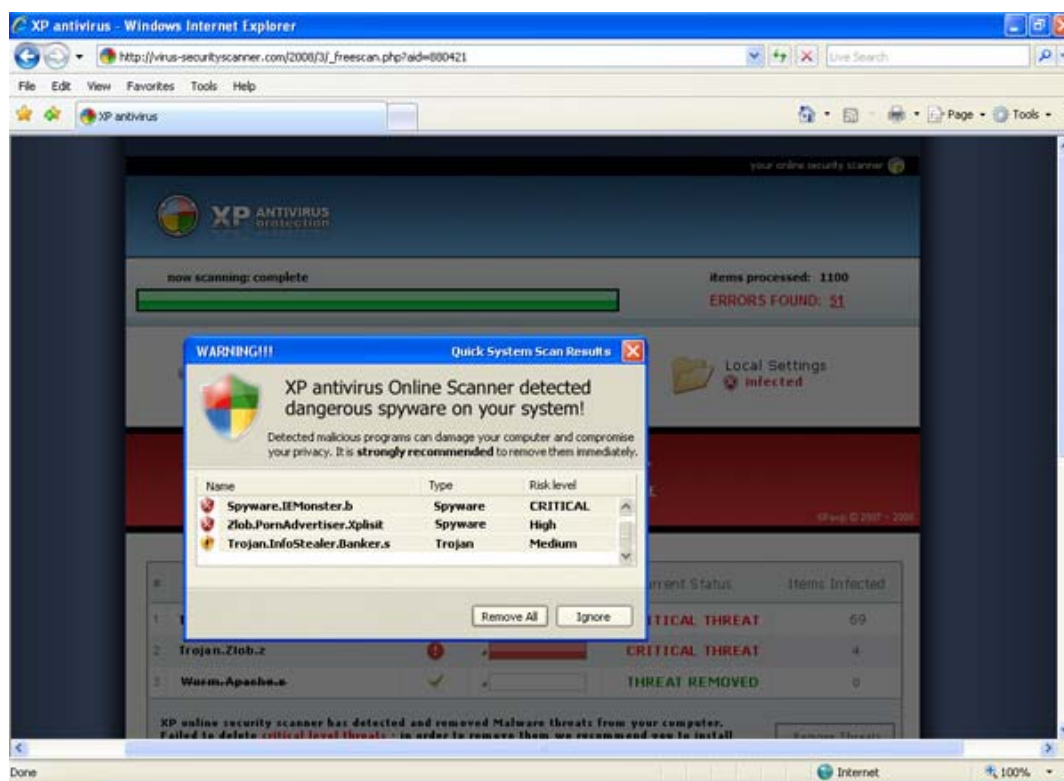


Figure 4 Fake Scan Results

Figure 4 is the same as Figure 1, but this time with the proper chrome as this virtual machine was running Windows XP. It turns out that the malware actually failed to install on Windows Vista (no, I did not file a bug with the authors to get that fixed), so I went back to Windows XP for my testing.

The page in Figure 4 is mostly just a composite of several images. The scan itself is a javascript that draws the progress bar. The file list that it iterates through when it performs the fake scan is a list of 1,100 names in a file called fileslist.js. That file also contains the 14 fake pieces of malware that it "discovers."

The warning dialog itself is a GIF image called popup3.gif. Virtually all areas of the page, including popup3.gif, are linked through an on-click event to a function called onloadExecutable(), which looks like this:

```
function onloadExecutable()
{
  dat=new Date(1214372723);
  var dlth=dat.getHours()-dat.getUTCHours();
  rrc = 1;
  location.href="../_download.php?aid=880421&dlth="+dlth;
};
```

This function does nothing more than trigger a download by setting the location of the browser to a script that initiates a download. The use of this design makes it harder to track down what they are doing since most forensics tools, such as wget, do not execute javascript. The objective, however, is quite clear: you are prompted to download something. The aid parameter is going to be appended to your download name as a version number. The time parameter does not seem to be used at all.

One very interesting behavior of popup3.gif is that the fake close button is actually linked to a special

warning. If you click that button, you get the warning in Figure 5.

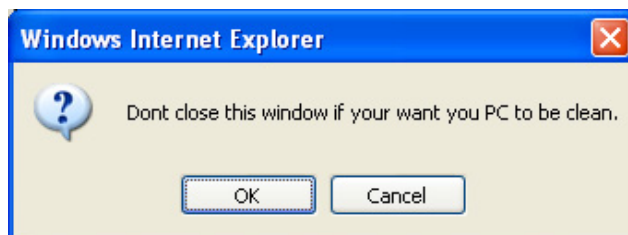


Figure 5 Closing one warning brings up another

If you click OK in Figure 5 it runs the `onloadExecutable()` function. If you click cancel or close it throws another warning, shown in Figure 6. That warning will run `onloadExecutable()` no matter what you do; whether you click the OK button or the red X to close it.



Figure 6 Closing that warning brings up one that gives you no options

Therefore, no matter what you do, you will be prompted to download a file. The file is: http://virus-securityscanner.com/2008/download/XPantivirus2008_v880421.exe. The v880421 part of the file is a fake version number which bubbled all the way from the original page. It does not seem to change very frequently. However, I tried a few hundred different numbers surrounding 880421 and most resulted in a valid download. Disturbingly, they all seem slightly different. It is possible that `download.php` runs the file through an obfuscator, but more than likely they have a few hundred different obfuscated versions of the same malware sitting on the server.

After downloading the file, I sent it to virustotal.com, a site that scans files on demand using a large number of reputable commercial anti-malware engines. The results varied a little depending on the day I tried it and which version of the file I sent them. For example, on June 24, only GData and Kaspersky detected the current version as malware. A version just a day older was also detected as malicious by AntiVir, eSafe, Sophos, and Webwasher-Gateway. The actual malware contained in the file is the Trojan-Downloader.Win32.FraudLoad.gen downloader trojan

Installing the Malware

The malware is actually quite well written, looking very professional. The installer starts out with a notification shown in Figure 7. It includes what appears to be a Windows compatibility logo, fake of course, and has a link to the terms and conditions.

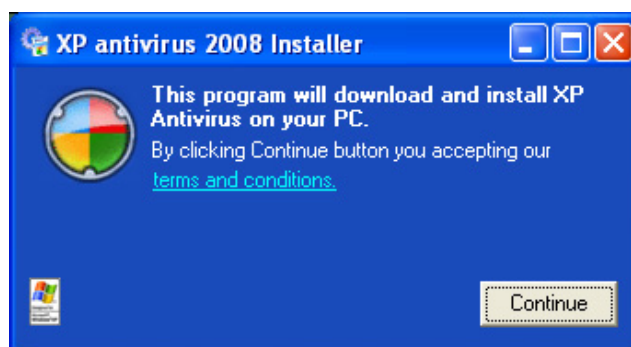


Figure 7 The installer looks very professional

The terms and conditions also look very professional. A snippet is shown in Figure 8.

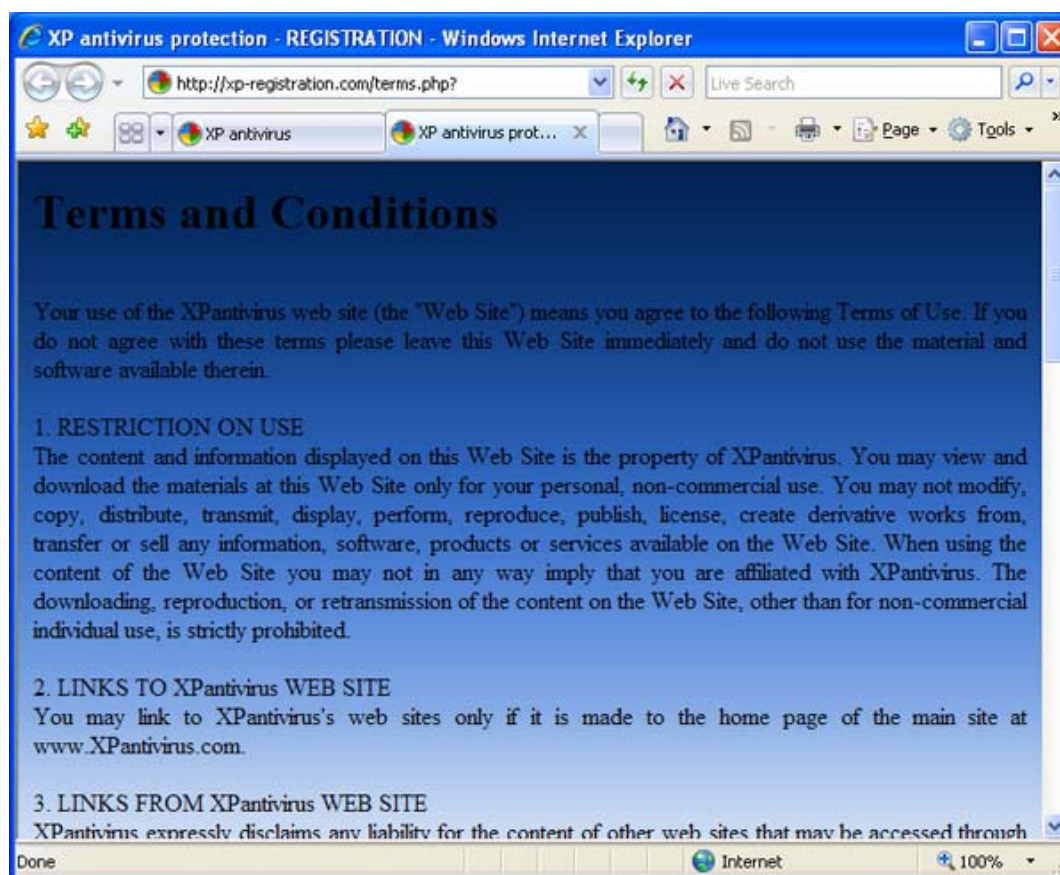


Figure 8 The malware comes with terms and conditions

The license agreement looks about like what you would expect from commercial software. Interestingly, however, it seems exclusively focused on the website, not on the software you are trying to install. It even tries to restrict how you can provide links to their site. That alone should be a reasonable hint, providing anyone actually ever reads license agreements.

The agreement also provides a link to the support site for the malware. A portion of the help file is shown in Figure 9.

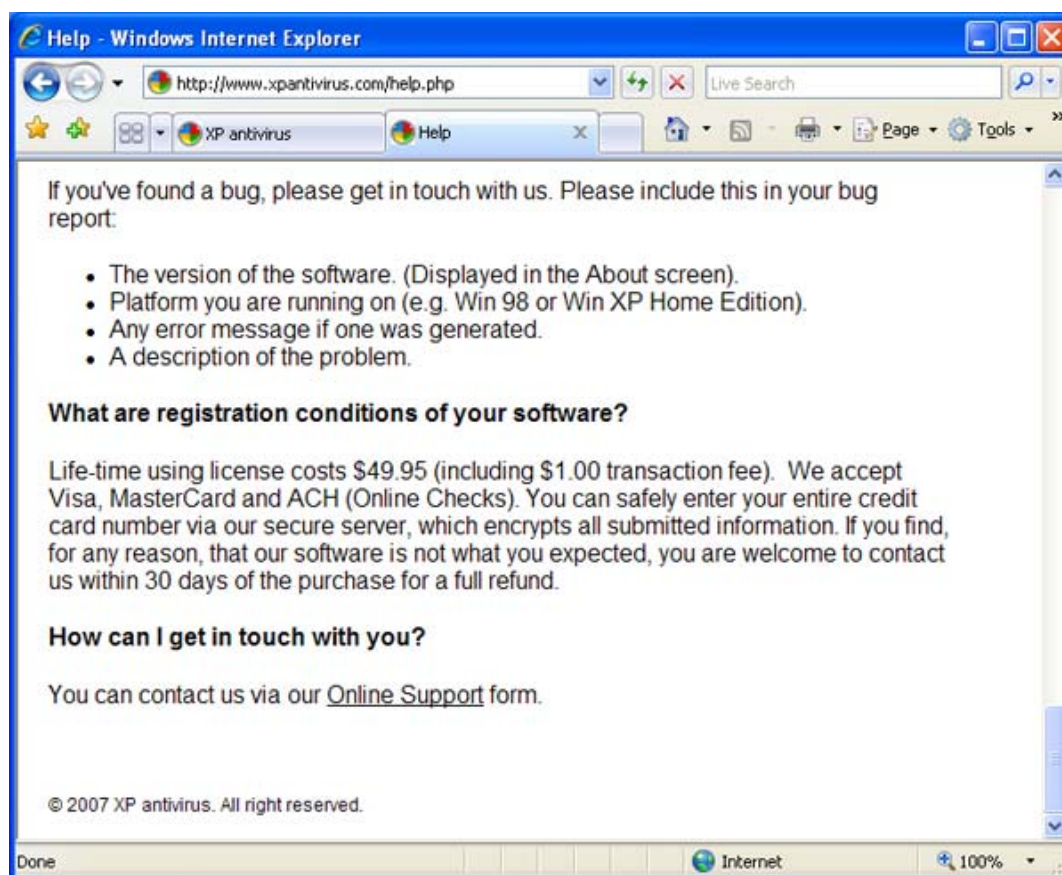


Figure 9 The malware has everything, including a help site

Once you know this is malware, the help site is almost comical. It has information about bug reporting, conspicuously lacking an actual method to submit bug reports. It makes it clear how much you will be charged to install the malware, and even uses the boilerplate language about how safe it is to submit your credit card to them because no criminals will be able to read the encrypted transmission; until it reaches the criminals who asked for it, of course. There is even a link to an online support forum, shown in Figure 10.



Figure 10 The malware has a support forum

The support forum looks well done, with mostly well designed graphics and the requisite list of cryptic malware names you find in the support forums for all anti-malware software. This list of malware is, of course, fake. However, it gives a nice view into what other sites might be associated with the same gang of criminals. Antispywareboss.com, antivirus-2008-pro.com, securityscannersite.com, winantispyware2008.com, and xpsecuritycenter.com are just some of the sites advertising solutions to W32.Trojan.Downloader.s. In fact, 411-spyware has a thread on that particular fake threat (<http://www.411-spyware.com/remove-w32-trojan-downloader-s>).

Sending Your Money to the Bad Guys

If you chose to actually pay for the software you will be directed to <https://secure.software-payment.com>. That site is hosted out of Bridgetown, Barbados. According to several websites, software-payment.com appears to be a bit of a favorite among those pushing fake anti-malware. [This forum thread](http://www.temerc.com/forums/viewtopic.php?p=3430848) (<http://www.temerc.com/forums/viewtopic.php?p=3430848>) has a list of other fake anti-malware that used it for their billing services.

The software costs \$49.95, as shown in Figure 9. However, when you try to register it you are also offered an upgrade to File Shredder 2008, for only \$39.95. It is not clear whether that upgrade destroys your data only locally, or whether, for that fee, the bad guys will destroy your data securely on their own servers after they use it to steal your identity and your money. You may also add premium support for \$24.95.

What It Installs

The first thing you will notice after installation is that you are presented with the Windows Security

Center, shown in Figure 11; except that it actually is not the Windows Security Center.

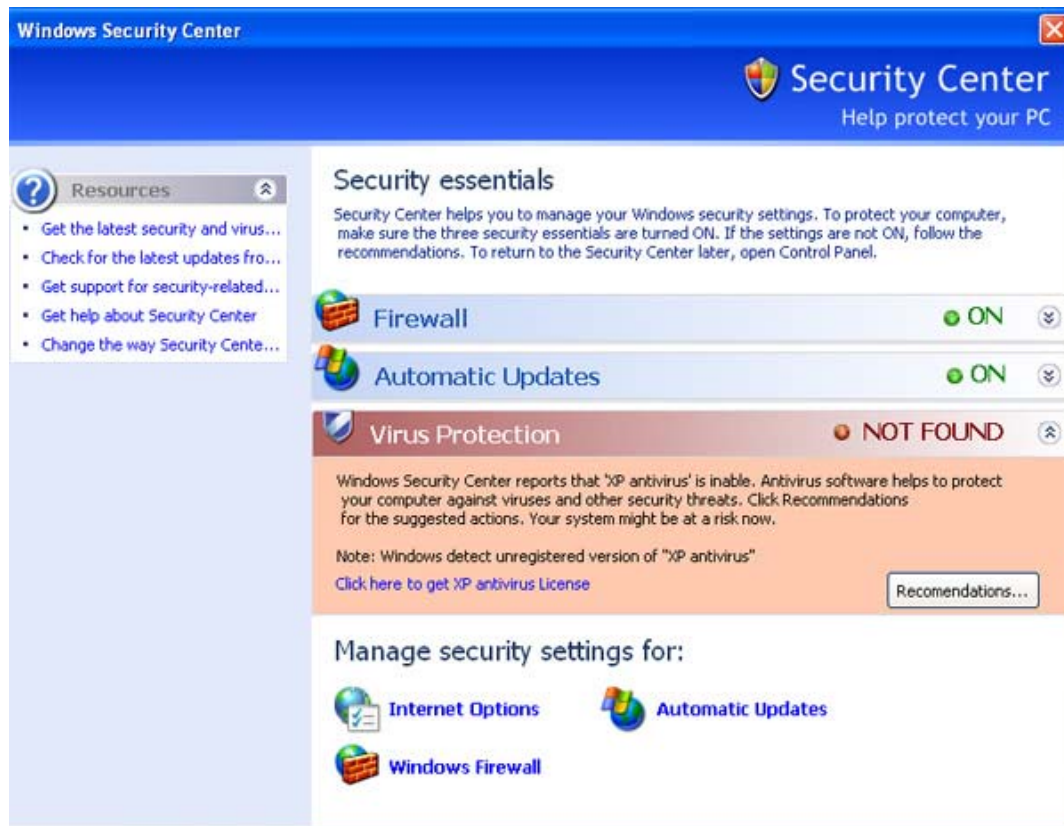


Figure 11 Fake Windows Security Center

Figure 11 shows a fake Windows Security Center. It looks very much like the real thing, shown in Figure 12 on the same computer, at the same time, for comparison purposes. Note that the real one does NOT detect the malware as a legitimate anti-virus program. The primary differences are twofold. First, the recommendations link in the fake one is linked to a dialog that will try, once again, to make you purchase the fake anti-malware. In the real one, it links to a help document explaining how to obtain anti-malware software.



Figure 12 Real Windows Security Center

The fake Windows Security Center also has a list of resources on the left hand side. However, all of them are linked to documents that entice you to pay for the malware. In the real one they link to real help files. It is likely that the criminals created the fake Windows Security Center so they could control exactly what you saw when you clicked on anything in it and link it to the ubiquitous purchase screen. The real Windows Security Center is still present on the computer. Notice the Control Panel in Figure 13.

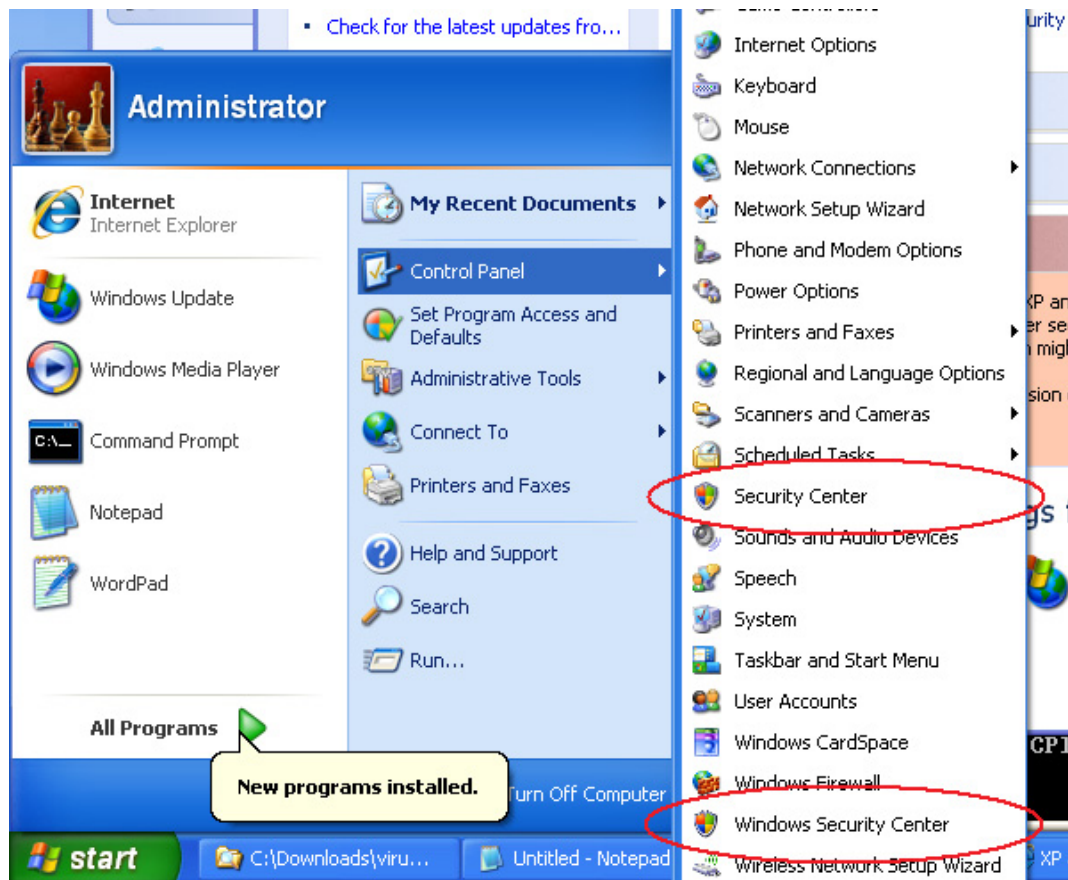


Figure 13 Fake Windows Security Center in the Control Panel

The real Windows Security Center is the one called just "Security Center" in the Control Panel. The fake one is the one called "Windows Security Center." In addition, the fake one identifies itself as "Windows Security Center" in the system tray. The real one identifies itself as "Security Alerts." It is probably safe to say that most users would be hard pressed to conclude that the real one was not the one called "Windows Security Center." Once again, it is a matter of telling real from fake, and in this case, unfortunately, the real thing, while there, is not very good at identifying itself as the real thing consistently.

If you leave the computer alone for a few minutes you will eventually get the first of many many popups of various kinds, shown in Figure 14.



Figure 14 The first of many warnings

The warning in Figure 14 is yet another attempt at getting you to send your money to the criminals. If you click the "Remove all threats now" button it will take you to a purchase screen. Interestingly, the "Continue unprotected" button does not take you there, breaking with the previous history. If you use that button you will start getting system tray popups. An example is shown in Figure 15.



Figure 15 One of several different scary looking system tray warnings

The malware uses several different system tray warnings. Another one is shown in Figure 16.

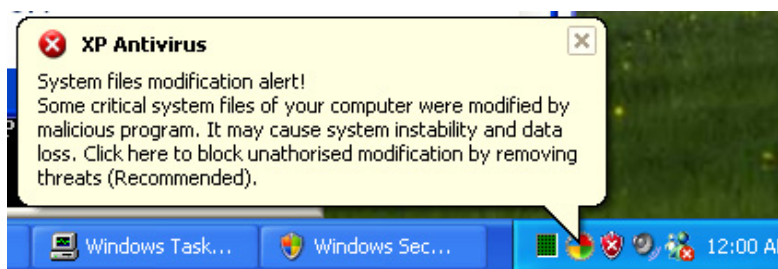


Figure 16 Another system tray warning

Interestingly, while virtually everything else the malware has shown us so far has been in flawless English, the system tray popups have grammatical mistakes and missing prepositions. More than likely this is indicative of collusion within a criminal gang to create the malware. The software and all the associated collateral is far too complex to be written by a single person in a reasonable time, so the source is likely a gang. The individual that wrote the system tray popups apparently did not receive the grammar tutorial the others did. Or, maybe, the system tray popups just were not part of the user acceptance testing plan.

At regular intervals you also get a strange corner popup, shown in Figure 17.



Figure 17 A corner popup

The corner popup also shows up in the region of the system tray but is just a window. It has an "Update Now" button that takes you to the purchase site. Once again, the malware is specifically designed to entice you to pay for it.

The application itself looks reasonably good. Figure 18 shows the main application window during a "scan."

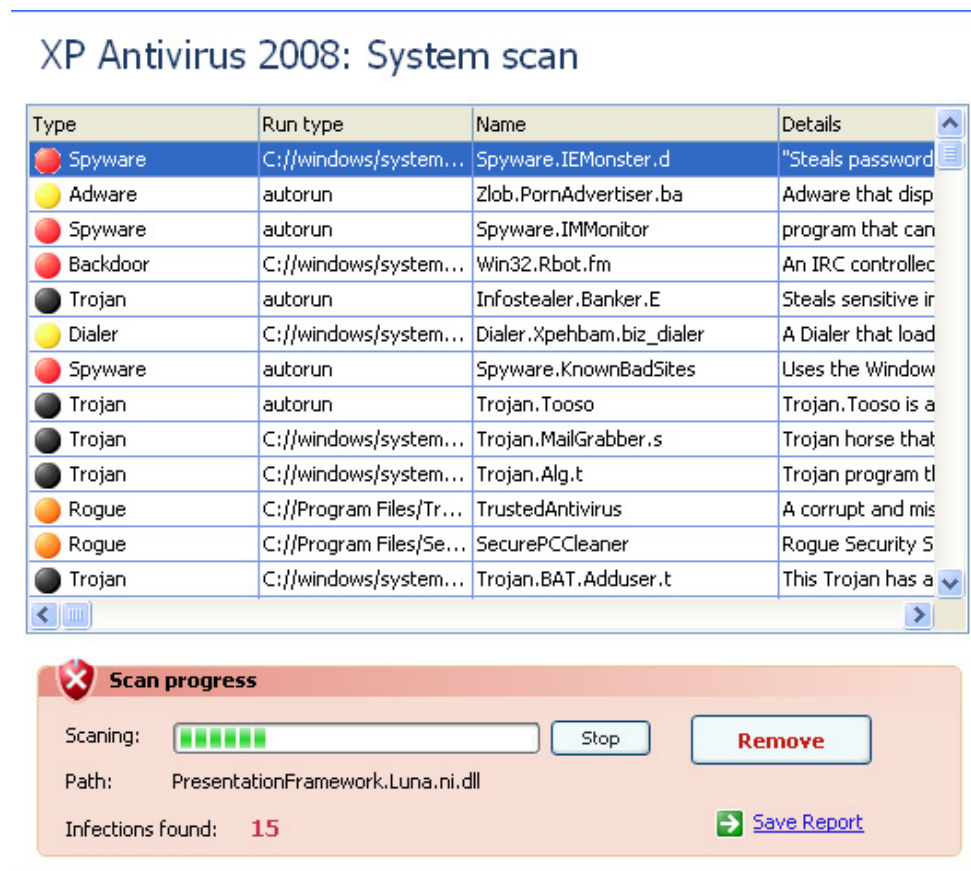


Figure 18 A scan of your system obviously finds many fake infections

If you compare Figure 18 to your average legitimate anti-malware suite you would probably be inclined to agree that this looks perfectly legitimate to most people. It finds bad stuff, which is good, and the bad stuff is sufficiently scary sounding to make me want to get it removed, even if it costs me \$49.95, plus the File Shredder 2008 license. Just in case that was not enough to entice me to purchase the malware, however, we also have the system status screen in Figure 19, which is designed to frighten you into compliance. By now you can probably guess where the "Update Now" button goes. There are at least four buttons in Figure 19 that lead to the "send us your money now" website. One can only marvel at how much better the criminals are at separating you from your money than the legitimate anti-malware vendors.

XP Antivirus 2008: Status



Protection level: low Low Medium High

Recommendation:
[Update antivirus](#)

Virus Protection NOT FOUND

Spyware Protection NOT FOUND

General Security NOT FOUND

Automatic Updating NOT FOUND

Scan Now
Check your computer for viruses and other threats

Update Now
Download the latest protection to help keep your PC safe

Last scan: **25.06.2008 00:06:11** Registration e-mail: **Unregistered**
Total scans: **2** Registration code:

Figure 19 The System Status screen is designed to be scary

Interestingly, in my testing, the malware did not actually take any malicious action beyond what I have documented here. I did not detect any attempts at stealing data, at installing additional malware, or at remote control. This could be for several reasons. The purpose may just be to get some of your money, and maybe a credit card number. Alternatively, it may be that the software is time-triggered to make it harder to analyze. Most analysts do not have the luxury to let it run continuously for weeks whereas the bad guys can easily wait that long for the payout. Finally, the software may include detection logic to discover that it is running in a virtual machine, causing it to forego some of the malicious actions it otherwise would. Such logic is becoming more common in malware as it makes it far more difficult for researchers to analyze the software.

Detection by Legitimate Software

As a final experiment I decided to see if I could remove the malware, or at least detect it, with legitimate anti-malware software. At first I attempted with the recently updated Microsoft Malicious Software Removal Tool (from June 24, 2008, the most recent available at the time I wrote this). It failed to detect the software.

Fortunately, other anti-malware software did detect it. Figure 20 shows the warning from [AVG Free](http://www.grisoft.com) (<http://www.grisoft.com>) when you attempt to open the Control Panel applet. AVG Free also threw a similar warning when I downloaded the installer.

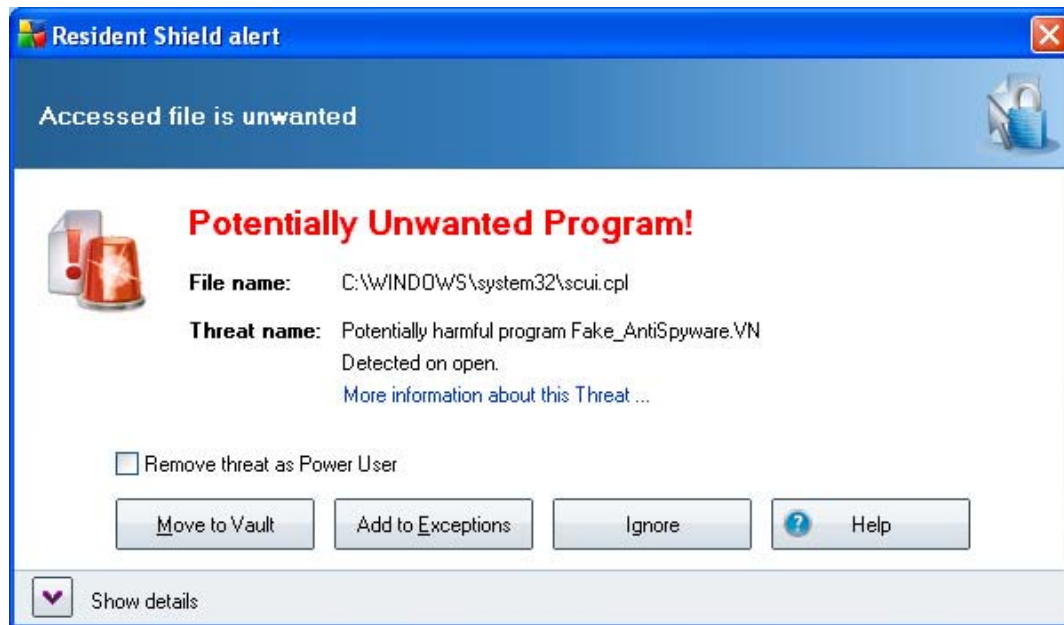


Figure 20 AVG Free detects the malware on open

AVG also detects the other vectors installed by the malware and very efficiently removes them for you, as shown in Figure 21. I did not test with any other anti-malware software. As the test results on Virus Total showed, the malware would probably be missed by at least some legitimate anti-malware software.

Scan is running

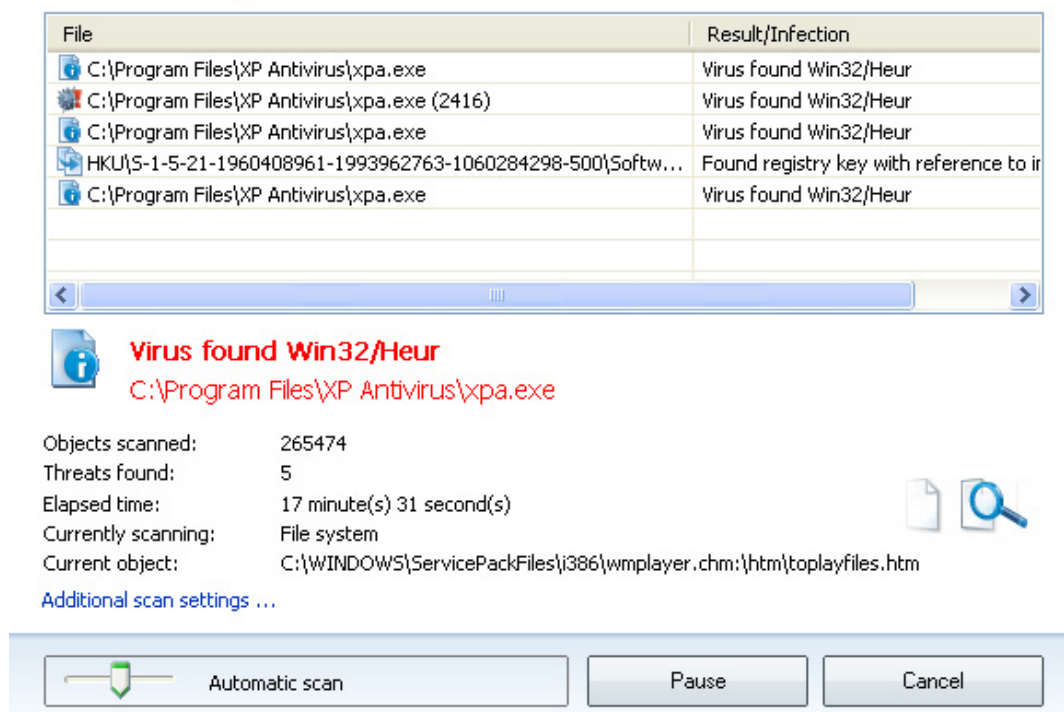


Figure 21 AVG Free removes the malware

Conclusion

This type of malware is very, very disturbing. One can only wonder how many users have been duped into installing ineffective security software, and what happened to their private information and credit card data when they paid for it. The presence of such software, and the overall very high quality of the ruse it presents, is frightening. More than likely, thousands of people have been fooled. In fact, this type of deception has been around for several years now, and it would not still be here if it did not work well.

This should serve as a dire warning to all: be extremely careful what you trust, and question everything that looks even remotely suspicious. For example, no website can run an anti-malware scan on your computer simply by your visiting the site. Any site that purports to do so is almost certainly run by criminal gangs.

No website should ever offer you to download an anti-malware package as soon as you visit the site. Any site that purports to do so is either run by criminal gangs or by an organization whose business practices are so deceptive that you should never consider doing business with it. A reputable site will present you with product information and then leave the downloading decision up to you, not force it upon you. No software that pushes the purchase decision so heavily in your face is likely to be legitimate.

Finally, learn just a little about how your computer looks normally so you can detect changes. The fake Windows Security Center is a very nice touch that could fool almost anyone except who doesn't pay attention to what the real one looks like and is called.

As for your anti-malware software, yes you need it. We all really do, at least on some computers. Advocating that you should stop using anti-malware software is irresponsible. If people were to actually take that advice, we would be overrun with malware in short order. You should definitely have anti-malware software on any computer that may come into contact with untrusted data and software.

However, do not just pick software because it tells you do pick it. Stick to the trusted brand names when it comes to anti-malware. And, if you get a download shoved down your computer when you visit a website, head over to [Virus Total](http://www.virustotal.com/) (<http://www.virustotal.com/>) and submit it for a scan. If it proves malicious, they will submit it to the anti-malware vendors for you. ®

Jesper M. Johansson is a Software Architect working on security software and is a contributing editor to *TechNet Magazine*. He holds a Ph.D. in Management Information Systems, has more than 20 years experience in security, and is a Microsoft Most Valuable Professional (MVP) in Enterprise Security. His latest book is the *Windows Server 2008 Security Resource Kit*.

Related stories

[Windows 7 UAC flaw silently elevates malware access](http://www.theregister.co.uk/2009/02/04/windows_uac_flaw/) (4 February 2009)

http://www.theregister.co.uk/2009/02/04/windows_uac_flaw/

[Scareware mongers hitch free ride on Microsoft.com and others](http://www.theregister.co.uk/2008/12/23/open_redirect/) (23 December 2008)

http://www.theregister.co.uk/2008/12/23/open_redirect/

[Microsoft: Malware for Windows on the rise](http://www.theregister.co.uk/2008/11/03/microsoft_intelligence_report/) (3 November 2008)

http://www.theregister.co.uk/2008/11/03/microsoft_intelligence_report/

[Dutch court convicts teens for stealing pixels](http://www.theregister.co.uk/2008/10/22/teens_sentenced_for_runescape_item_theft/) (22 October 2008)

http://www.theregister.co.uk/2008/10/22/teens_sentenced_for_runescape_item_theft/

[Scammers making '\\$15m a month' on fake antivirus](http://www.theregister.co.uk/2008/10/16/fake_av_scam/) (16 October 2008)

http://www.theregister.co.uk/2008/10/16/fake_av_scam/

[Washington and Microsoft declare war on scareware](http://www.theregister.co.uk/2008/09/29/scareware_monger_sued/) (29 September 2008)

http://www.theregister.co.uk/2008/09/29/scareware_monger_sued/

[\(Former\) gambling site worker cops to ID theft](http://www.theregister.co.uk/2008/09/23/gambling_site_fraud/) (23 September 2008)

http://www.theregister.co.uk/2008/09/23/gambling_site_fraud/

[Million dollar burnout features as malware lure](http://www.theregister.co.uk/2008/09/22/cash_pyre_malware_lure/) (22 September 2008)

http://www.theregister.co.uk/2008/09/22/cash_pyre_malware_lure/

[Scammers skirt spam shields with help from Adobe Flash](http://www.theregister.co.uk/2008/09/04/spammers_using_adobe_flash/) (4 September 2008)

http://www.theregister.co.uk/2008/09/04/spammers_using_adobe_flash/

[US data breaches booming in '08](http://www.theregister.co.uk/2008/08/27/itrc_data_breaches_2008_beat_2007/) (27 August 2008)

http://www.theregister.co.uk/2008/08/27/itrc_data_breaches_2008_beat_2007/

[Mystery web attack hijacks your clipboard](http://www.theregister.co.uk/2008/08/15/webbased_clipboard_hijacking/) (15 August 2008)

http://www.theregister.co.uk/2008/08/15/webbased_clipboard_hijacking/

[Crooks charge premium for filter-evading Trojan](http://www.theregister.co.uk/2008/07/18/limbo_trojan/) (18 July 2008)

http://www.theregister.co.uk/2008/07/18/limbo_trojan/

[Almost half of malicious sites tied to 10 networks](http://www.theregister.co.uk/2008/06/24/stopbadware_report/) (24 June 2008)

http://www.theregister.co.uk/2008/06/24/stopbadware_report/

[Web browsers face crisis of security confidence](http://www.theregister.co.uk/2008/06/23/marginal_browser_security_protections/) (23 June 2008)

http://www.theregister.co.uk/2008/06/23/marginal_browser_security_protections/

[Rare Mac Trojan exploits Apple vuln](http://www.theregister.co.uk/2008/06/23/mac_trojan/) (23 June 2008)

http://www.theregister.co.uk/2008/06/23/mac_trojan/

[Instant trojan to worm toolkit sighted](http://www.theregister.co.uk/2008/06/18/trojan_worm_toolkit/) (18 June 2008)

http://www.theregister.co.uk/2008/06/18/trojan_worm_toolkit/



© Copyright 1998–2009