Rogue Antivirus Dissected - Part 1

URL: http://www.secureworks.com/research/threats/rogue-antivirus-part-1

Date: October 21, 2008

Author: Joe Stewart

Introduction

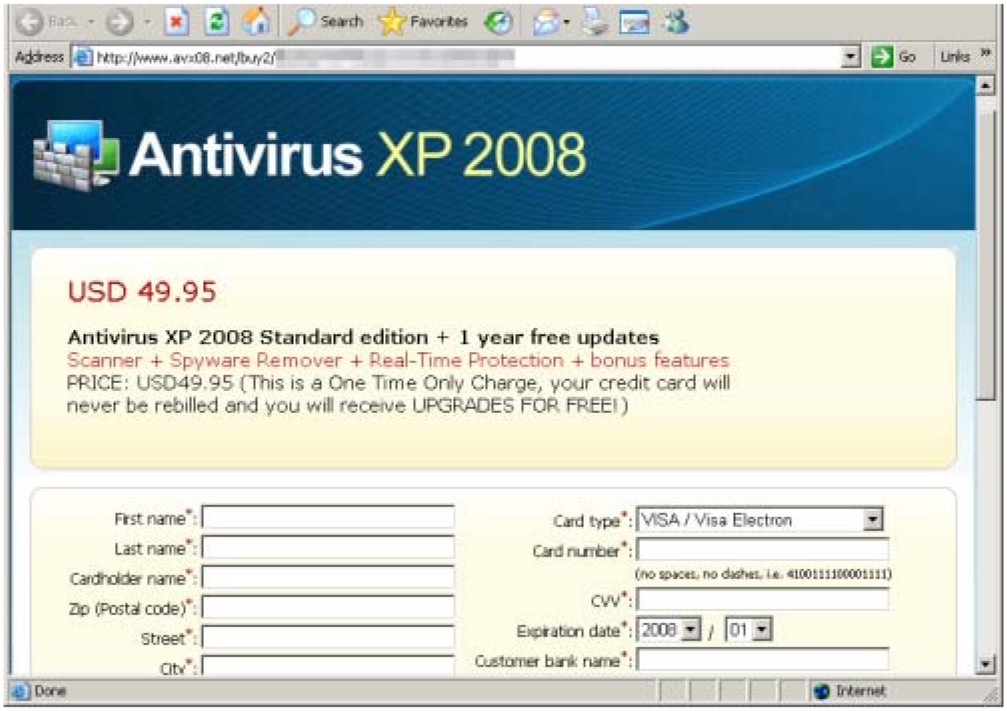
In a previous writeup, we detailed how the rogue antivirus program called "Antivirus XP 2008" infected a system and how it looks. But many questions remain, such as:

- Is there ANY antivirus capability in AV XP 2008 or is it 100% fraudulent?
- What happens when you pay to register the program?
- Where does the money go?
- Who is behind all this?
- How much money are they making?

In this analysis we will try to answer all of these questions.

The Registration Process

Once a victim of this software gets tired of the popups claiming they are infected with hundreds of viruses/trojans, they might click on the Registration tab of the program. When they do, the web browser displays the following page:



http://www.avx08.net/buy2/[redacted]

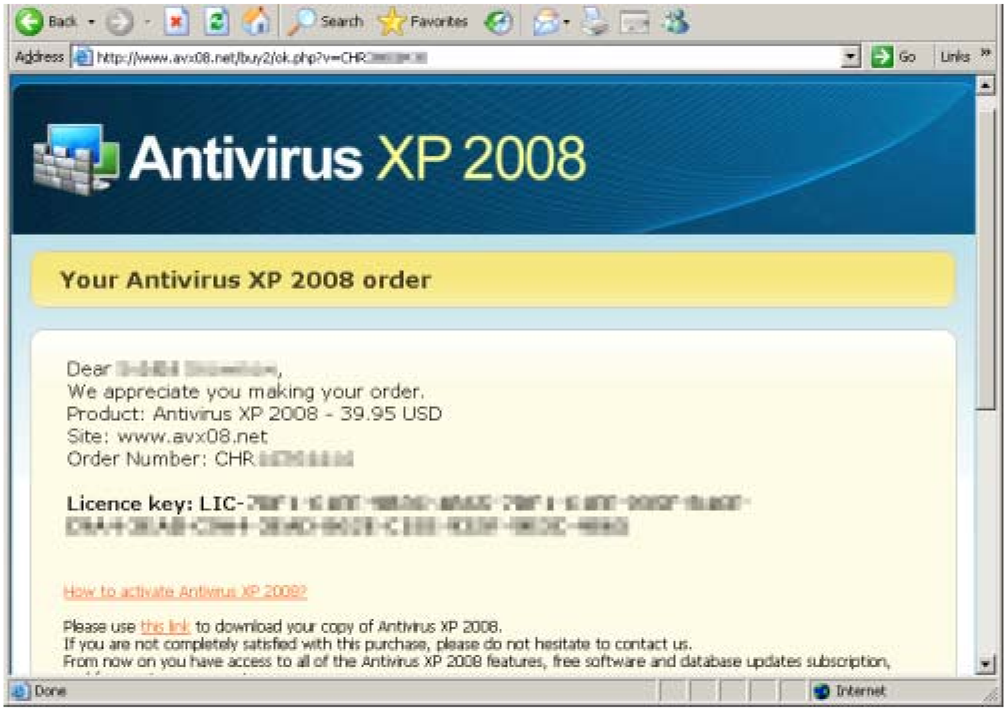
USD 49.95

Antivirus XP 2008 Standard edition + 1 year free updates
Scanner + Spyware Remover + Real-Time Protection + bonus features
PRICE: USD49.95 (This is a One Time Only Charge, your credit card will never be rebilled and you will receive UPGRADES FOR FREE!)

First name*:
Last name*:
Cardholder name*:
Zip (Postal code)*:
Street*:
City*:

Card type*: VISA / Visa Electron
Card number*:
(no spaces, no dashes, i.e. 4100111100001111)
CVV*:
Expiration date*: 2008 / 01
Customer bank name*:

If the user fills out the form and provides their credit card data, they will be taken to this subsequent page:



Your Antivirus XP 2008 order

Dear [redacted],
We appreciate you making your order.
Product: Antivirus XP 2008 - 39.95 USD
Site: www.avx08.net
Order Number: CHR[redacted]

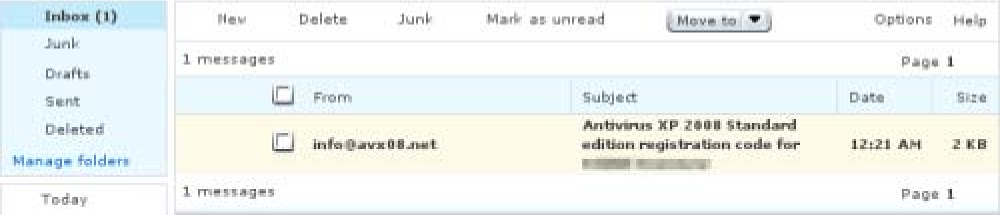
Licence key: LIC-[redacted]

How to activate Antivirus XP 2008?

Please use this link to download your copy of Antivirus XP 2008.
If you are not completely satisfied with this purchase, please do not hesitate to contact us.
From now on you have access to all of the Antivirus XP 2008 features, free software and database updates subscription,

In this case, the site hasn't been updated to reflect a new pricing plan - the displayed price was $49.95, but we were only charged $39.95. Of course, not everyone gets an unexpected discount - there are quite a few complaints on the Internet about people being overcharged when purchasing AV XP 2008 and other similar "scareware" products.

We even received an email with our registration code:

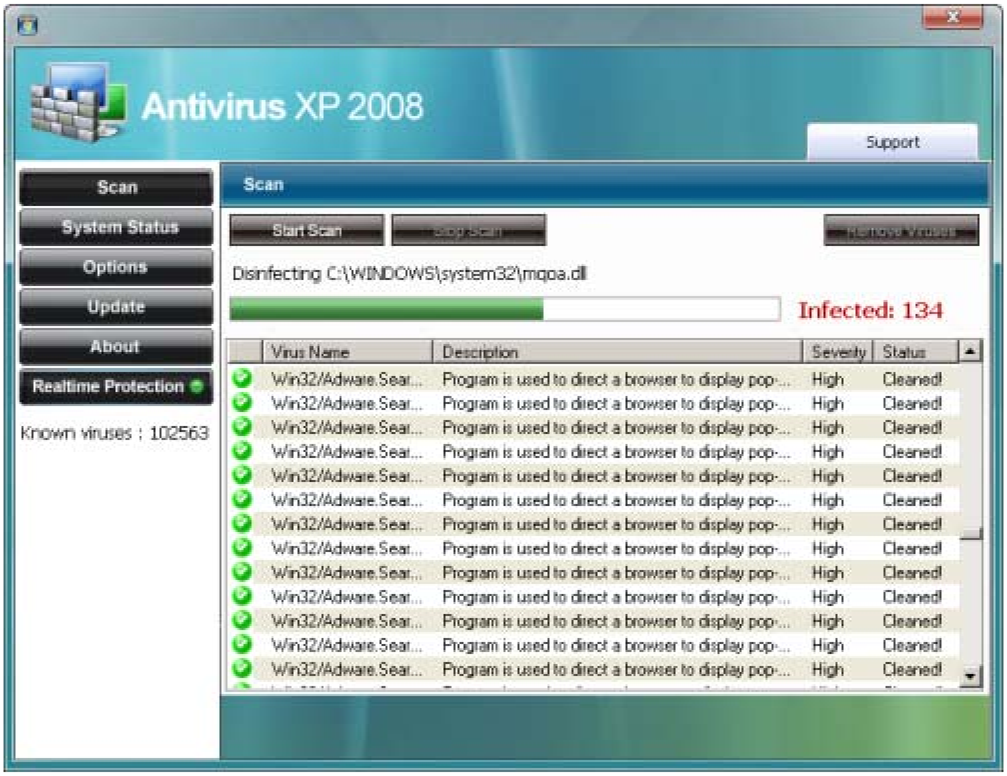


1 messages Page 1

	From	Subject	Date	Size
□	info@avx08.net	Antivirus XP 2008 Standard edition registration code for [redacted]	12:21 AM	2 KB

1 messages Page 1

Once the program was activated, it proceeded to pretend to disinfect the 309 threats it claimed to have found on a brand-new installation of Windows:



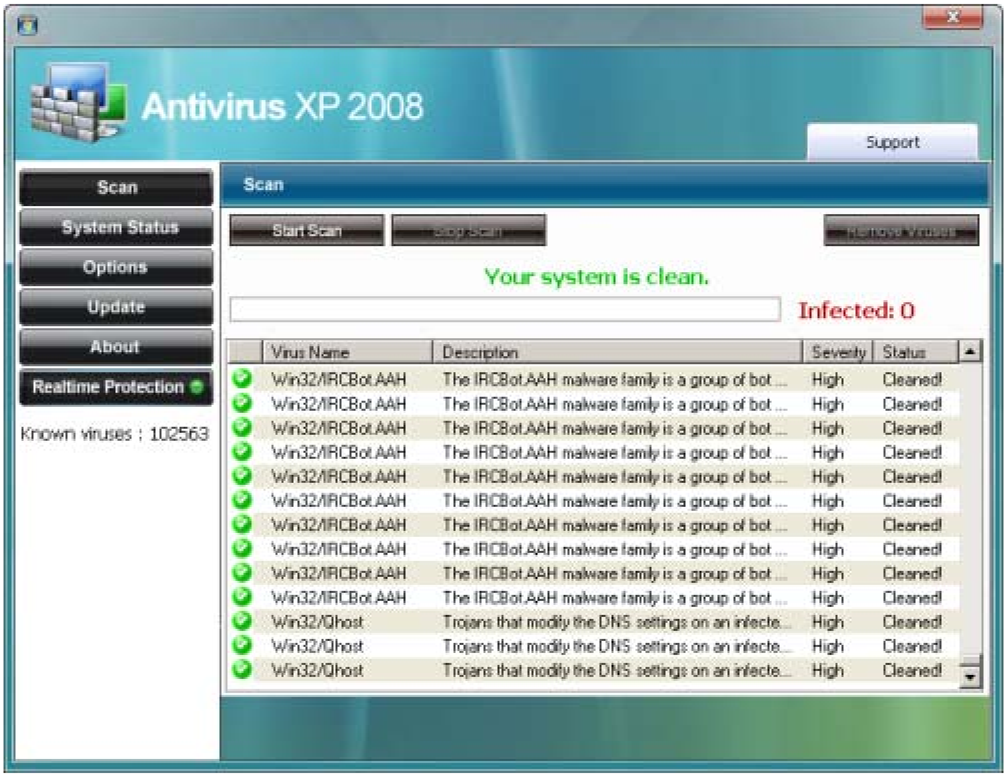
Scan

Known viruses : 102563

Disinfecting C:\WINDOWS\system32\mqoa.dll

Infected: 134

	Virus Name	Description	Severity	Status
✓	Win32/Adware.Sear...	Program is used to direct a browser to display pop-...	High	Cleaned!
✓	Win32/Adware.Sear...	Program is used to direct a browser to display pop-...	High	Cleaned!
✓	Win32/Adware.Sear...	Program is used to direct a browser to display pop-...	High	Cleaned!
✓	Win32/Adware.Sear...	Program is used to direct a browser to display pop-...	High	Cleaned!
✓	Win32/Adware.Sear...	Program is used to direct a browser to display pop-...	High	Cleaned!
✓	Win32/Adware.Sear...	Program is used to direct a browser to display pop-...	High	Cleaned!
✓	Win32/Adware.Sear...	Program is used to direct a browser to display pop-...	High	Cleaned!
✓	Win32/Adware.Sear...	Program is used to direct a browser to display pop-...	High	Cleaned!
✓	Win32/Adware.Sear...	Program is used to direct a browser to display pop-...	High	Cleaned!
✓	Win32/Adware.Sear...	Program is used to direct a browser to display pop-...	High	Cleaned!
✓	Win32/Adware.Sear...	Program is used to direct a browser to display pop-...	High	Cleaned!
✓	Win32/Adware.Sear...	Program is used to direct a browser to display pop-...	High	Cleaned!
✓	Win32/Adware.Sear...	Program is used to direct a browser to display pop-...	High	Cleaned!



Scan

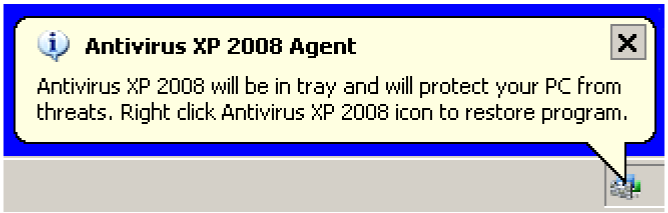
Known viruses : 102563

Your system is clean.

Infected: 0

	Virus Name	Description	Severity	Status
✓	Win32/IRCBot.AAH	The IRCBot.AAH malware family is a group of bot ...	High	Cleaned!
✓	Win32/IRCBot.AAH	The IRCBot.AAH malware family is a group of bot ...	High	Cleaned!
✓	Win32/IRCBot.AAH	The IRCBot.AAH malware family is a group of bot ...	High	Cleaned!
✓	Win32/IRCBot.AAH	The IRCBot.AAH malware family is a group of bot ...	High	Cleaned!
✓	Win32/IRCBot.AAH	The IRCBot.AAH malware family is a group of bot ...	High	Cleaned!
✓	Win32/IRCBot.AAH	The IRCBot.AAH malware family is a group of bot ...	High	Cleaned!
✓	Win32/IRCBot.AAH	The IRCBot.AAH malware family is a group of bot ...	High	Cleaned!
✓	Win32/IRCBot.AAH	The IRCBot.AAH malware family is a group of bot ...	High	Cleaned!
✓	Win32/IRCBot.AAH	The IRCBot.AAH malware family is a group of bot ...	High	Cleaned!
✓	Win32/IRCBot.AAH	The IRCBot.AAH malware family is a group of bot ...	High	Cleaned!
✓	Win32/Qhost	Trojans that modify the DNS settings on an infecte...	High	Cleaned!
✓	Win32/Qhost	Trojans that modify the DNS settings on an infecte...	High	Cleaned!
✓	Win32/Qhost	Trojans that modify the DNS settings on an infecte...	High	Cleaned!

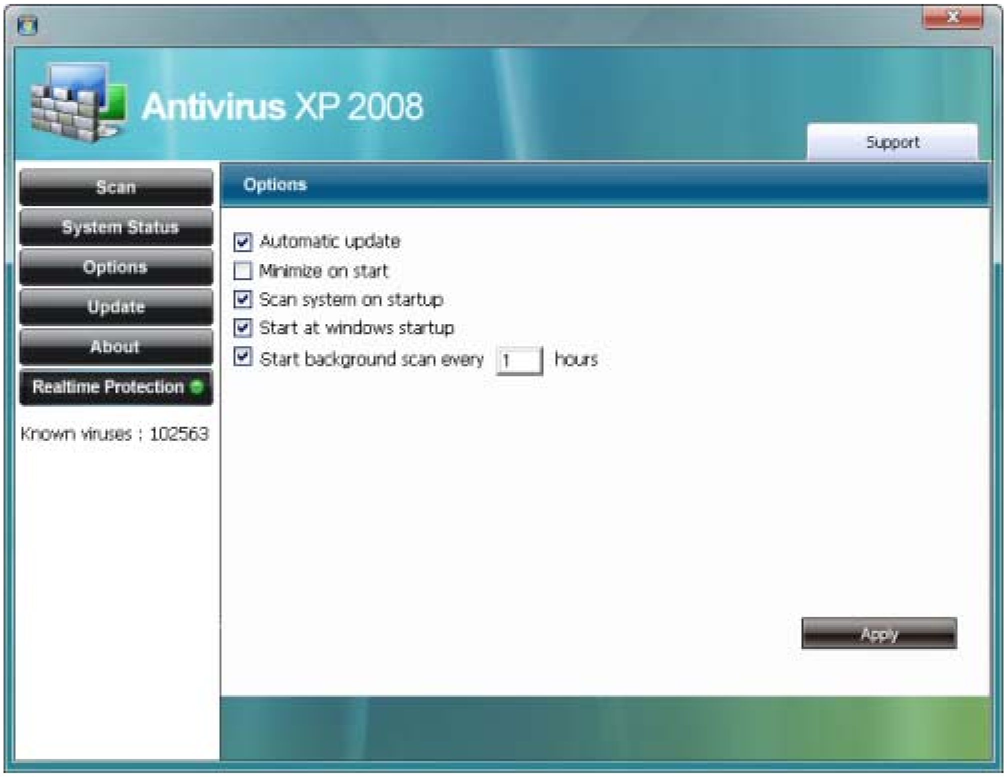
The urgent tray tooltip warnings were replaced with the following:



Antivirus XP 2008 Agent

Antivirus XP 2008 will be in tray and will protect your PC from threats. Right click Antivirus XP 2008 icon to restore program.

Previously greyed out, the options to stop AV XP 2008 from running at startup are now enabled:



Known viruses : 102563

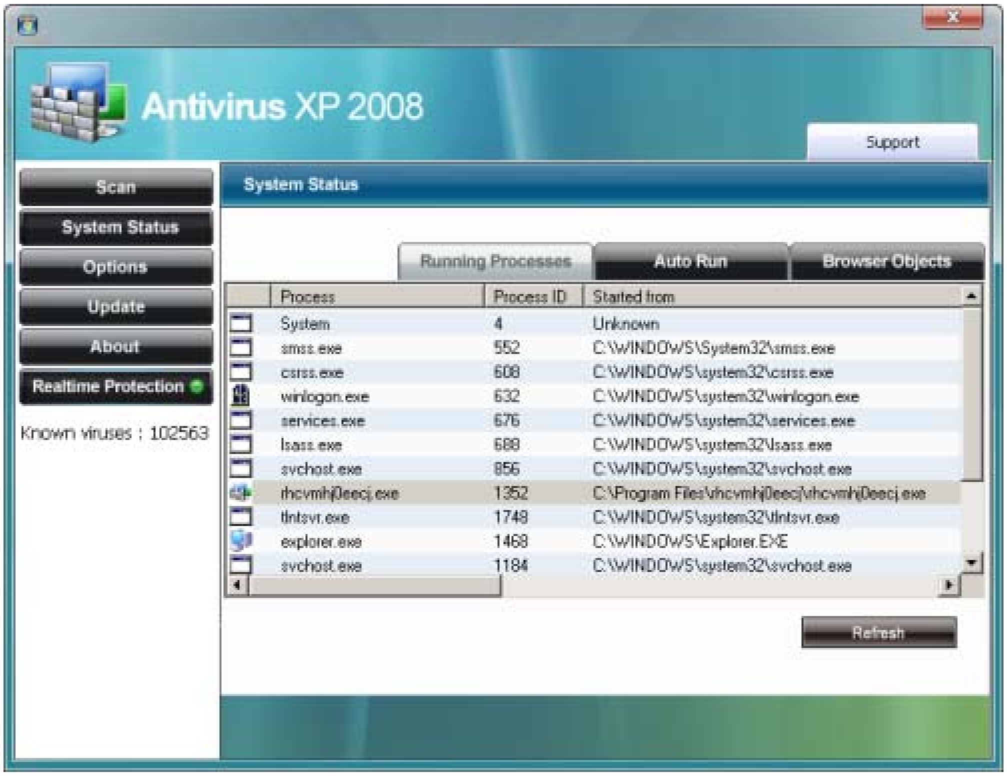
Options

☑ Automatic update
☐ Minimize on start
☑ Scan system on startup
☑ Start at windows startup
☑ Start background scan every 1 hours

Unchecking all options on this page will finally cause AV XP 2008 from popping up constantly. The warning on the desktop background wallpaper will disappear, and the fake bluescreen-of-death screensaver will be disabled, and the desktop properties tabs for changing the wallpaper and screensaver are restored. So paying for the program will make it stop being such a nuisance. But does the program have any function other than tricking the user into paying a hefty fee to get rid of its popups?

Functionality

As it turns out, AV XP 2008 does have some rudimentary anti-malware functionality. The System Status tab has a working task manager that will allow the user to view and kill processes (including AV XP 2008 itself). There is also an editor to allow the user to disable and quarantine Browser Helper Object and CurrentVersion\Run entries in the registry. So theoretically, the program could be used to manually disable some basic types of malware. However, it's a far cry from what a real Antivirus does, and all of these abilities are available in many other free programs.



Known viruses : 102563

Process	Process ID	Started from
System	4	Unknown
smss.exe	552	C:\WINDOWS\System32\smss.exe
csrss.exe	608	C:\WINDOWS\system32\csrss.exe
winlogon.exe	632	C:\WINDOWS\system32\winlogon.exe
services.exe	676	C:\WINDOWS\system32\services.exe
lsass.exe	688	C:\WINDOWS\system32\lsass.exe
svchost.exe	856	C:\WINDOWS\system32\svchost.exe
rhcvmhj0eecj.exe	1352	C:\Program Files\rhcvmhj0eecj\rhcvmhj0eecj.exe
tlntsvr.exe	1748	C:\WINDOWS\system32\tlntsvr.exe
explorer.exe	1468	C:\WINDOWS\Explorer.EXE
svchost.exe	1184	C:\WINDOWS\system32\svchost.exe

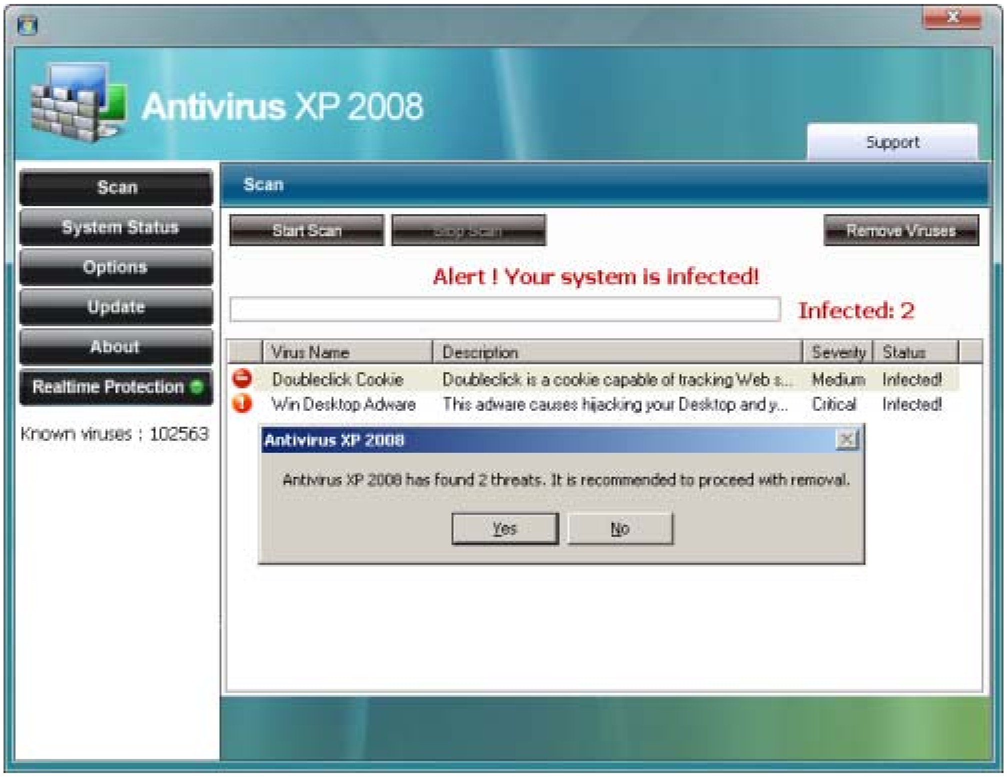
There is even a virus definitions file (named database.dat) shipped with AV XP 2008, which is decidedly small (1701 bytes). It is really just a ZIP file containing a file called compress.dat (8623 bytes). This file contains information about 17 different threats, including names, descriptions, registry keys and filenames. The actual list of threats and their descriptions as taken from the dat file is shown in the table below:

Name of Threat	Description of Threat
VIRUS.Krnl33	Description of the virus
VIRUS.Krnl32	Description of the virus
Trojan.Virupdate	Updates viruses on your computer
Spyware.BlueScreen	Heuristic trojan and malware loader, that runs third party illegal software.
Trojan.InternetUpdate	Heuristic trojan and malware loader, that runs third party illegal software.
Browser Hijaker Pro	This fraudware hijacks your browser and change homepage and searchpage. Capable of showing fraud popup advertisements and fake warnings and alerts.
Trojan VirDown	Provides remote access to your PC without your notice. Also performs SPAM and DDoS.
Trojan VX Downloader 2	Provides remote access to your PC without your notice. Also performs SPAM and DDoS.
Doubleclick Cookie	Doubleclick is a cookie capable of tracking Web site visitors and their personal favors.
Linker Adware	This badware will show fake and fraud advertisements on any web sites you surf
Complexel Trojan	Heuristic trojan and malware loader, that runs third party illegal software.
Win Desktop Adware	This adware causes hijacking your Desktop and you will face desktop ads popping up on your computer.
KillingBugs	This badware will show fake and fraud advertisements on any web sites you surf
Fraudware.SpyShredder	False-positive results produced by this rogue antispyware applications is just the thing that makes users to buy them.
Fraudware.MalwareCrush	False-positive results produced by this rogue antispyware applications is just the thing that makes users to buy them.
Fraudware.X-P-Antivirus	False-positive results produced by this rogue antispyware applications is just the thing that makes users to buy them.
XP Cleaner	False-positive results produced by this rogue antispyware applications is just the thing that makes users to buy them.

This is actually a pretty humorous list, considering that many of the threats purported to be cleaned by AV XP 2008 are actually older versions of itself.

To test whether or not these threats are actually detected and removed by AV XP 2008, we surfed to doubleclick.com (loading a DoubleClick cookie onto our machine) and manually created a file in C:\WINDOWS\system32 named ctfmona.exe, a known filename associated with malware (and one of the filenames listed in the AV XP 2008 compress.dat file), containing only the word "test" instead of executable content.

Surprisingly, Antivirus XP 2008 actually detected and removed both, but only after running a manual scan - we were able to add both files to the system despite the "Realtime Protection" feature:



Known viruses : 102563

Alert ! Your system is infected!

Infected: 2

	Virus Name	Description	Severity	Status
⊖	Doubleclick Cookie	Doubleclick is a cookie capable of tracking Web s...	Medium	Infected!
!	Win Desktop Adware	This adware causes hijacking your Desktop and y...	Critical	Infected!

Antivirus XP 2008

Antivirus XP 2008 has found 2 threats. It is recommended to proceed with removal.

Obviously the detection of the ctfmona.exe file was done solely based on the filename instead of any kind of binary signatures, so it's not a complex detection/disinfection engine. But it does posess at least some of the functionality it claims to. However it appears that it only detects and removes 17 relatively minor threats, not 102,563 known viruses as the interface seems to suggest.

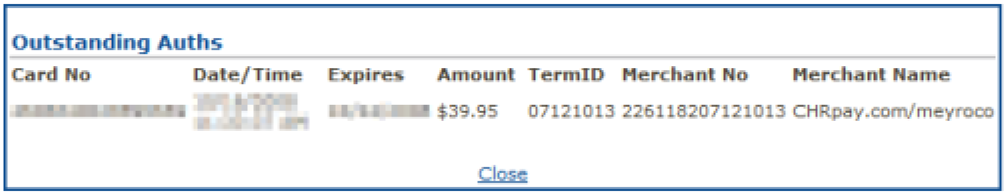
The addition of very simplistic antivirus functionality gives the authors of AV XP 2008 plausible deniability. If challenged in a court of law they might try to claim the program is not truly fraudulent - after all, it can clean computers of at least a few malicious programs. Maybe those 309 threats it said it found on a clean system were just false-positives - and who *doesn't* have problems with false-positives when writing malware-detection programs? Since it has been shown in various tests that modern antivirus engines fail to detect 80% of new malware, the AV XP 2008 authors could claim their software is only 20% less effective than major brand antivirus programs! What judge could argue with that logic?

The Money Trail

Once you become a registered customer, you get access to a "VIP support" page located at http://[site name]/vipsupport/. At this page you can request a phone support number by entering a valid registered email address. However, that interface claimed that our email address was invalid (despite the fact that the software license key had been sent to that same address by the registration system).

You can also request a refund, however the refund terms are confusing at best, and lead one to believe it is unlikely that any refund will ever be given. Of course, if paying by credit card, it is possible to issue a chargeback and obtain a refund from the credit card company, who will take the money back from the merchant. Users of debit cards are not so lucky, however.

The refund page makes reference to a service called "billinghost.net" supposedly doing the credit card processing. We checked the account statement for the card we used to make the purchase to see who was actually listed as the merchant:



Outstanding Auths

Card No	Date/Time	Expires	Amount	TermID	Merchant No	Merchant Name
[redacted]	[redacted]	[redacted]	$39.95	07121013	226118207121013	CHRpay.com/meyroco

In this case, it appears that CHRpay.com was used to make the charge to our card - this is ChronoPay, a large credit card payment processor located in the Netherlands (with offices in Russia and Latvia). ChronoPay provides small businesses with the ability to take credit cards without having to have their own merchant account. ChronoPay was at one time the credit card processor for allofmp3.com, a well-known and controversial music download site in Russia.

In this case, the username of the ChronoPay customer receiving the money for XP AV 2008 purchases appears to be "meyroco", which is probably just one of many accounts that have been created by the AV XP 08 author(s). It doesn't tell us much about who is behind this software, but that information can already be found on the Internet with a little sleuthing. In the next part of this article, we will take an inside look at the affiliate program that is driving the installation of AV XP 08 and related rogue antimalware products.

>> Part 2 of Rogue Antivirus