Anatomy of a Hack, 2008

Jesper M. Johansson, Ph.D.
Jesper_m_johansson@hotmail.com

Key Takeaways

- Thieves have no honor
- Preying on people is easy
- The ill-informed are the ones that are fooled
Ancient History
Internet Worm

The Plagues
Code Red, Nimda ...
When Money Enters Into It…

Our story begins
Checked out the site

THE MALICIOUS SITE

Demo
Initial Warning

Windows Internet Explorer

ATTENTION! If your computer is infected, you could suffer data loss, enable PC behavior, PC freezes and crashes.
Detect and remove viruses before they damage your computer!
XP Antivirus will perform a quick and 100% FREE scan of your computer for Viruses, Spyware and Adware.
Do you want to install XP Antivirus to scan your computer for malware now? (Recommended)

OK Cancel

It's totally safe!

Windows Internet Explorer

XP Antivirus will scan your system for threats now.
Please select "RUN" or "OPEN" when prompted to start the installation.
This file has been digitally signed and independently certified as 100% free of viruses, adware and spyware.

OK
No, don't do that!

You're in trouble.
But we can help

Surrender and accept terms

If you fulfill the following conditions as a cause for a refund, you can claim for refund for following months or within the first five days of the current month.

A. Monthly subscription customers may only claim for refund for following months or within the first five days of the current month.

B. The customer can record software downloaded from Internet to CD or any other media for non-commercial purposes.

C. Refunds will not be given because of wrong or improper software settings set. Instructions on correct settings are described in the days trial procedure.

D. We declare the functionality of all Software we sell. Refunds will not be granted on the grounds of the Software not performing any function it was not originally intended to perform.

E. Customers cannot demand a refund on Software if the problem is not related to that particular software. We declare the functionality of all Software we sell. Refunds will not be granted on the grounds of the Software not performing any function it was not originally intended to perform.

F. Disassemble, modify, translate, make any attempt to discover the source code of Antivirus XP 2008, or create derivative works of Antivirus XP 2008.

G. If the customer has problems downloading Antivirus XP 2008, he or she may contact the customer support service which will provide them with an alternative method within 72 hours after the complaint was filed. Declaring a refund is NOT possible without installing and a 7-day trial period.

H. Partial refunds for defective Antivirus XP 2008 may be granted if the product has been acquired as part of a bundled purchase.

I. You may not:

   A. use one copy of Antivirus XP 2008 on one (1) single computer during subscription period;
   B. make one copy of Antivirus XP 2008 for archival purposes, or copy the Antivirus XP 2008 onto the hard disk of your computer and retain the original for archival purposes;
   C. use Antivirus XP 2008 on a network, provided that You have a licensed copy of Antivirus XP 2008 for each computer that can access Antivirus XP 2008 over that network;
   D. after written permission from AntivirusXP2008.com, transfer Antivirus XP 2008 on a permanent basis to another person or entity, provided that You retain no copies of Antivirus XP 2008 and the transferee agrees to the terms of this license;
   E. be informed of any changes or updates regarding the Antivirus XP 2008 by e-mail or any other contact method available.

   You may not:

   A. use one copy of Antivirus XP 2008 on one (1) single computer during subscription period;
   B. use Antivirus XP 2008 on a network, provided that You have a licensed copy of Antivirus XP 2008 for each computer that can access Antivirus XP 2008 over that network;
   C. use a previous version or copy of Antivirus XP 2008 after You have received a disk replacement set or an upgraded version. Upon upgrading the Software, all copies of the prior version must be destroyed;
   D. use a later version of the Antivirus XP 2008 than is provided herewith unless You have purchased upgrade insurance or have otherwise separately acquired the right to use such later version;
   E. be informed of any changes or updates regarding the Antivirus XP 2008 by e-mail or any other contact method available.

   You may:

   A. use one copy of Antivirus XP 2008 on one (1) single computer during subscription period;
   B. make one copy of Antivirus XP 2008 for archival purposes, or copy the Antivirus XP 2008 onto the hard disk of your computer and retain the original for archival purposes.

   Your rights and obligations with respect to the use of this Software are as follows:

   You must:

   A. be informed of any changes or updates regarding the Antivirus XP 2008 by e-mail or any other contact method available.
   B. Our 24/7 customer support service should be contacted for any troubleshooting. Customer support service should be informed in the event the customer's system crashed for any reason, in order for the customer to be entitled to claim a refund. If the support team is not contacted, a refund will NOT be made. This reduces all problems to technical difficulties which will be researched and solved.
   C. Some of our products may be unsuited to run with other software. We reserve the right to change for or remove any conflicting software. In the event the customer's system crashed for any reason, in order for the customer to be entitled to claim a refund. If the support team is not contacted, a refund will NOT be made. This reduces all problems to technical difficulties which will be researched and solved.
   D. We are not liable if the customer's system was restored or repaired and a refund will NOT be made.
   E. We are not liable if the customer's system was restored or repaired and a refund will NOT be made.
   F. We are not liable if the customer's system was restored or repaired and a refund will NOT be made.
   G. We are not liable if the customer's system was restored or repaired and a refund will NOT be made.
   H. We are not liable if the customer's system was restored or repaired and a refund will NOT be made.
   I. We are not liable if the customer's system was restored or repaired and a refund will NOT be made.
   J. We are not liable if the customer's system was restored or repaired and a refund will NOT be made.
   K. We are not liable if the customer's system was restored or repaired and a refund will NOT be made.
Third half of license agreement

4. Content Updates

Certain AntivirusXP2008.com products may utilize content that is updated from time to time (antivirus products utilize updated virus definitions; content filtering products utilize updated URL lists; firewall products utilize updated firewall rules; vulnerability assessment products utilize updated vulnerability data, etc.; collectively, these are referred to as “Content Updates”). The software looks for updates automatically, if not configured otherwise.

Being invisible to the user, certain AntivirusXP2008.com products run its processes to ensure the entire protection against menaces. The process is active even after the scan and clean session has been completed in the background to protect your PC and be able to always seek, detect, stop, or remove incoming errors or threats. The processes launch themselves at start up automatically, if not configured otherwise.

All updates are provided “as is” without express or implied warranty of any kind and AntivirusXP2008.com cannot be held responsible for the failure to provide such updates.

5. Limited Warranty

AntivirusXP2008.com does not warrant that Antivirus XP 2008 will meet Your requirements or that operation of Antivirus XP 2008 will be uninterrupted or that Antivirus XP 2008 will be error-free for specific environment.

You assume responsibility for selecting the software to achieve your intended results, and for the use and the results obtained from the software.

AntivirusXP2008.com and its suppliers disclaim all warranties, express or implied, including but not limited to warranties related to: non-infringement, lack of viruses, accuracy or completeness of responses or results, implied warranties or merchantability and fitness for a particular purpose.

The above warranty is exclusive and in lieu of all other warranties, whether express or implied, including the implied warranties of merchantability, fitness for a particular purpose and noninfringement of intellectual property rights.

This warranty gives you specific legal rights. You may have other rights, which vary from state to state and country to country.

6. Disclaimer of Damages

SOME STATES AND COUNTRIES, INCLUDING MEMBER COUNTRIES OF THE EUROPEAN ECONOMIC AREA, DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW AND REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL ANTI-VIRUSXP.COM OR ITS LICENSORS BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INDIRECT OR SIMILAR DAMAGES, INCLUDING ANY LOST PROFITS OR LOST DATA ARISING OUT OF THE USE OR INABILITY TO USE ANTI-VIRUS XP 2008 Software. IN NO CASE SHALL ANTI-VIRUSXP.COM OR ITS LICENSORS’ LIABILITY EXCEED THE PRICE OF PURCHASE OF ANTI-VIRUS XP 2008. The disclaimers and limitations set forth above will apply regardless of whether You accept Antivirus XP 2008.
Look, we even have support

SAMPLE APPLICATION
Is This Real or Fake?

Security essentials
Security Center helps you manage your Windows security settings. To help protect your computer, make sure the above security essentials are enabled. If the settings are not OK, follow the recommendations. To return to the Security Center, tap or click Control Panel. What’s new in Windows 7: help.protectmycomputer.com

Firewall
ON

Automatic Updates
ON

Virus Protection
NOT FOUND

Windows define the antivirus software on this computer. Antivirus software helps protect your computer against viruses and other security threats. Use recommended or supported antivirus you can take. Is this antivirus software help protect my computer?

Note: Windows does not detect all antivirus programs.

Manage security settings for:
Internet Options  Windows Firewall
Automatic Updates

Is This Real or Fake?
They're both there

Pay us or we'll pop you

WARNING! 66 infections found!!!
Unwanted software (malware) or tracking cookies have been found during last scan. It is highly recommended to remove it from your computer.

- Lost Documents and Settings
- Permanent Data Loss
- System not starting up
- System slowdown and crashes
- Loss of Internet Connection
- Infecting other computers on your network

Remove all threats now  Continue unprotected
More popups

The app itself
SAMPLE APPLICATION 2

It continually evolves
Antispyware Master

Variant on Sept. 23
Intercepts Regular Traffic

Insecure Internet activity. Threat of virus attack

Due to insecure Internet browsing your PC can easily get infected with viruses, worms and trojans without your knowledge, and that can lead to system slowdowns, freezes and crashes. Also insecure Internet activity can result in revealing your personal information. To get full advanced real-time protection for PC and Internet activity, register your antivirus software.

We recommend you to protect your PC now and continue safe Internet browsing.

- Click here to get full advanced real-time protection and continue browsing.
- Continue to the website unprotected (not recommended).

Demo
Sept. 23 Purchase Site

Charges

➤ $82.90 each from:

<table>
<thead>
<tr>
<th>COUNTRY</th>
<th>DATE/TIME</th>
<th>MERCHANT NAME/CITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>RU</td>
<td>09/09 20:23</td>
<td>SPYWARE-SHOP2.CO</td>
</tr>
<tr>
<td>LV</td>
<td>09/09 20:23</td>
<td>WAV2008.COM RIGA</td>
</tr>
<tr>
<td>RU</td>
<td>09/09 20:27</td>
<td><a href="http://WWW.SPYWARE-MALL">WWW.SPYWARE-MALL</a></td>
</tr>
<tr>
<td>LV</td>
<td>09/09 20:28</td>
<td>WAV2008.COM RIGA</td>
</tr>
<tr>
<td>RU</td>
<td>09/09 20:27</td>
<td>SPYWARE-SHOP6.CO</td>
</tr>
</tbody>
</table>
A fake Windows Security Center, called "Windows Security Center"

The BSOD screen saver

Use of rogue ActiveX controls

Attempted launching of real ActiveX controls with known vulns

IE add-ins to intercept browsing to other web sites and present a virus infection warning instead
Tricks They Are Known To Be Using

- Immediate removal of the original infector
- Several layers of indirection in the execution
- Bin packing the malware
- Requiring connectivity to a rogue web site to execute infector
- Versions that appear to be built on the fly based on the exact link the victim followed to get the original infector
- Repositioning the browser windows to fool the user about where they are

Key Takeaways

- Thieves have no honor
- Preying on people is easy
- The ill-informed are the ones that are fooled