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
<table>
<thead>
<tr>
<th>Ancient History</th>
<th>Internet Worm</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>The Plagues</th>
<th>Code Red, Nimda</th>
</tr>
</thead>
</table>
When Money Enters Into It…

Our story begins
Checked out the site

THE MALICIOUS SITE

THE MALICIOUS SITE
Initial Warning

Windows Internet Explorer

ATTENTION! If your computer is infected, you could suffer data loss, enable PC behaviour, PC freezes and crashes.

Detect and remove viruses before they damage your computer!

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
ANTIVIRUS XP 2008 LICENSE AGREEMENT


By accepting this License Agreement you give your consent that the details of your credit card are being retained within the entire period of subscription.

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

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;
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; and
D. use Antivirus XP 2008 for archival purposes in a manner consistent with the terms of this License Agreement.

You may not:
A. 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;
B. sublicense, rent or lease any portion of Antivirus XP 2008; reverse engineer, decompile, disassemble, modify, translate, make any attempt to discover the source code of Antivirus XP 2008, or create derivative works;
C. 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;

We have the right to uninstall incompatible products. We will notify our customers before uninstalling such products. In such cases, if the customer is not satisfied, the customer can request a refund.

2. Refunds Policy

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 software team is not contacted, a refund will NOT be made.

This reduces all problems to technical difficulties which will be researched and solved.

AntivirusXP2008.com is not responsible for any help the customer gets from third parties. We will not give a refund if the customer is not satisfied with the service provided.

Some of our products may be unsuited to run with other software. In such cases, the customer must be satisfied with the software. In such cases, the customer must be satisfied with the software.

The usage of Antivirus XP 2008 requires the uninstallation of products which represent a risk to the system.

Customers cannot demand a refund on Software if the problem is not related to that particular software. We declare the liability of all services and Software. You will not be granted on the grounds of the Software not performing any function it was not intended to perform. The issues 1 & 2 customer should notify AntivirusXP2008.com of the issue by phone call to +33 01 51 10 23 90.

We are not liable if the customer's system was restored or repaired and a refund will NOT be made.

AntivirusXP2008.com cannot be held responsible for actions performed by the customer when not using our Software.

The customer must contact the customer support service which will provide a full explanation about this within 72 hours after the complaint was filed. Declaring a refund is NOT possible without installing and a 7-day trial procedure.

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

Refunds will not be given because of wrong or improper software settings or instructions on correct settings are described in the manual and can be also requested through the Software's web site or Customer Support Service.

In a few cases, the customer may desire a refund for reasons other than the Software's defects. In such cases, we will only refund to the extent possible. Antivirus XP 2008 is not to be used for data recovery or any other technical purpose.
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: (i) the Software will meet your requirements; (ii) the operation of the Software will be uninterrupted or error-free; (iii) any faults in the Software will be corrected; (iv) the Software will be compatible with any third party software or hardware; (v) the Software will operate in the user’s 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.

ANTIVIRUS XP 2008 software automatically adds AntivirusXP2008.com sites to Internet Explorer trusted zone.

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 below 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 shall AntivirusXP2008.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 Antivirus XP 2008 even if AntivirusXP2008.com has been advised of the possibility of such damages.

In no case shall AntivirusXP2008.com or its licensors’ liability exceed the price of purchase of Antivirus XP 2008. The disclaimers and limitations set forth above will apply regardless of whether you accept Antivirus XP 2008.

If you have trouble, we can help
Look, we even have support.

Sample Application

Demo
Is This Real or Fake?

Windows Security Center

Security essentials

Security Center helps you to manage your Windows security settings. To protect your computer, make sure that these security essentials are enabled. Always turn on the recommended settings. To return to the Security Center, open Control Panel.

Firewall
- ON

Automatic Updates
- ON

Virus Protection
- NOT FOUND

Windows Security Center reports that 'SP antivirus' is not enabled. Antivirus software helps to protect your computer against viruses and other security threats. Click 'Recommendations' for the suggested actions. Your antivirus is not the latest version.

Note: Windows does not detect all virus programs.

Manage security settings for:
- Internet Options
- Windows Firewall
- Automatic Updates
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 this website unprotected (not recommended).
$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