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 It...
Our story begins

A Comment has been posted to Jesper's Blog: **Hey, Mozilla: Quotes Are Not Legal in a URL** by **southwest-airlines**:

[link_to_blog_post]

This Comment was Not Published (Spam Score: 3).

Use the links below to publish or delete this comment:

[Approve]  [Delete]
Checked out the site

XP antivirus - Windows Internet Explorer

[Image of a computer window showing a scan result]

**WARNING!!!**

XP antivirus Online Scanner detected dangerous spyware on your system!

Detected malicious programs can damage your computer and compromise your privacy. It is **strongly recommended** to remove them immediately.

**Name**               | **Type** | **Risk level**
-----------------------|----------|------------------
Spyware.IEMonster.b    | Spyware  | CRITICAL         
Zlob.PornAdvertiser.Xplisit | Spyware  | High            
Trojan.InfoStealer.Banker.s | Trojan  | Medium          

[Buttons: Remove All, Ignore]
THE MALICIOUS SITE
ATTENTION! If your computer is infected, you could suffer data loss, erratic PC behaviour, 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)
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!

Windows Internet Explorer

Don't close this window if you want your PC to be clean.

OK  Cancel
You're in trouble

Harmful and malicious software detected. These programs may damage your computer and steal your private information. Online Security Scanner requires XP antivirus components to repair your computer. Please click OK to download and install XP antivirus components.
But we can help
Terms and Conditions

Your use of the XPantivirus web site (the "Web Site") means you agree to the following Terms of Use. If you do not agree with these terms please leave this Web Site immediately and do not use the material and software available therein.

1. RESTRICTION ON USE
The content and information displayed on this Web Site is the property of XPantivirus. You may view and download the materials at this Web Site only for your personal, non-commercial use. You may not modify, copy, distribute, transmit, display, perform, reproduce, publish, license, create derivative works from, transfer or sell any information, software, products or services available on the Web Site. When using the content of the Web Site you may not in any way imply that you are affiliated with XPantivirus. The downloading, reproduction, or retransmission of the content on the Web Site, other than for non-commercial individual use, is strictly prohibited.

2. LINKS TO XPantivirus WEB SITE
You may link to XPantivirus's web sites only if it is made to the home page of the main site at www.XPantivirus.com.

3. LINKS FROM XPantivirus WEB SITE
XPantivirus expressly disclaims any liability for the content of other web sites that may be accessed through

Surrender and accept terms
ANTIVIRUS XP 2008 LICENSE AGREEMENT

IMPORTANT: PLEASE READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE USING ANTIVIRUS XP 2008. ANTIVIRUSXP2008.COM AND/OR ITS SUBSIDIARIES ARE WILLING TO LICENSE THE SOFTWARE TO YOU AS THE INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING ANTIVIRUS XP 2008 (REFERENCED BELOW AS "YOU" OR "YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND ANTIVIRUSXP2008.COM BY CLICKING ON THE "AGREE" OR "YES" BUTTON OR OTHERWISE INDICATING ASSENT ELECTRONICALLY, OR LOADING THE SOFTWARE, YOU AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS, CLICK ON THE "I DO NOT AGREE", "NO" BUTTON, OR OTHERWISE INDICATE REFUSAL; MAKE NO FURTHER USE OF THE SOFTWARE, AND CONTACT THE CUSTOMER SUPPORT TEAM.

1. License

The software which accompanies this license (collectively the "Software") is the property of AntivirusXP2008.com or its licensors and is protected by copyright law. While AntivirusXP2008.com continues to own Antivirus XP 2008, You will have certain rights to use Antivirus XP 2008 after Your acceptance of this license. This license governs any releases, revisions or enhancements to Antivirus XP 2008 that AntivirusXP2008.com may furnish to You.

In case you keep using our product within 7 days following the expiration of the one-year period of subscription, you are automatically charged for the product cost.

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 this 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. 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. copy the printed documentation which may accompany Antivirus XP 2008;
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 from Antivirus XP 2008;
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:
2. Refunds Policy

B. Our 24/7 customer support service should be contacted for any troubleshooting. Customer support service should be informed of 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. AntivirusXP2008.com is not responsible for any help the customer gets from third party technicians or any work done by the customer are made at his or her risk.

C. Some of our products may be unsuited to run with other software. We have the right to uninstall incompatible products. We will notify our customers before uninstalling such products and will not be responsible for any regulations or removal of conflicting software.

Coexistence of some products may lead to many unsatisfactory effects as well as to slow the customer’s system. That is why the usage of Antivirus XP 2008 requires the uninstallation of products which represent a risk to the system.

D. 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. The issues the customer faced are related to the interaction of the Software with different systems or other software. AntivirusXP2008.com is not responsible for any harmful interactions.

In this case the technical department will analyze the customer’s system data and report possible reasons for the problem.

E. We are not liable if the customer’s system was restored or repaired and a refund will NOT be made in such a case.

In a few cases, product-related Antivirus XP 2008 cannot deal with overloaded and damaged systems. In such cases, AntivirusXP2008.com is not responsible.

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

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-days trial procedure.

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

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

J. Refunds will not be given for not providing software burned on CD or any other media. There is no charge for CD cost or shipping. The customer can record software downloaded from Internet to CD or any other media for non-commercial purposes.

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

Refunds will not be given for previous months.
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.

AntivirusXP2008 setup procedure may uninstall some products or some components in order to avoid their incompatibility with the Software being installed.

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 WILL 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.

If you have trouble we can help

If you've found a bug, please get in touch with us. Please include this in your bug report:

- The version of the software. (Displayed in the About screen).
- Platform you are running on (e.g. Win 98 or Win XP Home Edition).
- Any error message if one was generated.
- A description of the problem.

What are registration conditions of your software?

Life-time using license costs $49.95 (including $1.00 transaction fee). We accept Visa, MasterCard and ACH (Online Checks). You can safely enter your entire credit card number via our secure server, which encrypts all submitted information. If you find, for any reason, that our software is not what you expected, you are welcome to contact us within 30 days of the purchase for a full refund.

How can I get in touch with you?

You can contact us via our Online Support form.
Look, we even have support.
Is This Real or Fake?

Security Center helps you to manage your Windows security settings. To protect your computer, make sure the three security essentials are turned ON. If the settings are not ON, follow the recommendations. To return to the Security Center later, open Control Panel.

Firewall
ON

Automatic Updates
ON

Virus Protection
NOT FOUND

Windows Security Center reports that 'XP antivirus' is unable. Antivirus software helps to protect your computer against viruses and other security threats. Click Recommendations for the suggested actions. Your system might be at a risk now.

Note: Windows detect unregistered version of "XP antivirus"
Click here to get XP antivirus License

Manage security settings for:

Internet Options
Automatic Updates
Windows Firewall
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
Demo

SAMPLE APPLICATION 2
It continually evolves
Antispyware Master

Online protection against malicious software

Antivirus scanner (quick scan starting)

Attention! Scanner has performed fast system scan. That means that not all entries were checked and possibly not all infected objects were found. It is recommended to download the program and implement full system scan. Download AntispywareMaster now

Progress 100%

Scanning drmpost.ai

Folder Directories Threat type

Windows Internet Explorer

Your computer has been running slower than normal, it may be infected with Viruses, Adware or Spyware.

AntiSpywareMaster will perform a quick and completely FREE scan of your system for malicious programs.

Download AntiSpywareMaster for FREE now!

Download anti-virus program - Windows Internet Explorer
Variant on Sept. 23
Sept. 23 software

Antivirus XP 2008 has found 1346 threats. It is recommended to proceed with removal.

Yes  No
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 slowdown, 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).
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 slowdown, 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).
Demo
Sept. 23 Purchase Site

Antivirus XP 2008

USD 39.95

Antivirus XP 2008 Standard edition + 1 year free updates
Scanner + Spyware Remover + Real-Time Protection + bonus features
PRICE: USD 39.95 (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): 
State: 
City: 
Country: United States
Email: 
Phone: 

Card type: VISA / Visa Electron
Card number: (no spaces, no dashes, i.e. 4000011111111111)
CVV: 
Expiration date: 2008 / 01
Customer bank name: 
Customer service phone: 

BUY

Instant Access, Discreet Billing, Secure Procedure by conveniently using our Online Credit Card Option.

5 good reasons to buy now:
- 24/7 qualified customer support service
- Progressive technology in action

System Information
- Antivirus has found 2346 viruses on your computer. It is recommended to decontaminate files as soon as possible.
$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>
Domain Name: a-vxp2008.com
Record created: 2008/9/16
Record expired: 2009/9/16

Domain servers in listed order:

Administrat:
name-- DNS MANAGER
country-- CN
organization-- ABSOLUTE CORP. LTD.
province-- Hongkong
city-- Hongkong
address-- FLAT/ROOM B 8/F CHONG MING BUILDING 72 CHEUNG SHA WAN RD KL
postalcode-- 999077
telephone-- +00.85223192933
fax-- +00.85223195168
E-mail-- a-3450400547301@absolute.com

Technical Contact:
name-- DNS MANAGER
organization-- ABSOLUTE CORP. LTD.
country-- CN
province-- Hongkong
city-- Hongkong
address-- FLAT/ROOM B 8/F CHONG MING BUILDING 72 CHEUNG SHA WAN RD KL
postalcode-- 999077
telephone-- +00.85223192933
fax-- +00.85223195168
E-mail-- a-3450400547301@absolute.com

Domain Name: G04SCF7.NET

Registrant:
PrivacyProtect.org
Domain Admin     (contact@privacyprotect.org)
P.O. Box 97
Note - All Postal Mails Rejected, visit Privacyprotect.org
Moergestel
null, 5066 ZH
NL
Tel. +45.36946676

Creation Date: 03-Sep-2008
Expiration Date: 03-Sep-2009

Domain servers in listed order:
ns1.2ru.us
ns3.2ru.us

Administrative Contact:
PrivacyProtect.org
Domain Admin     (contact@privacyprotect.org)
P.O. Box 97
Note - All Postal Mails Rejected, visit Privacyprotect.org
Moergestel
null, 5066 ZH
NL
Tel. +45.36946676
- 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