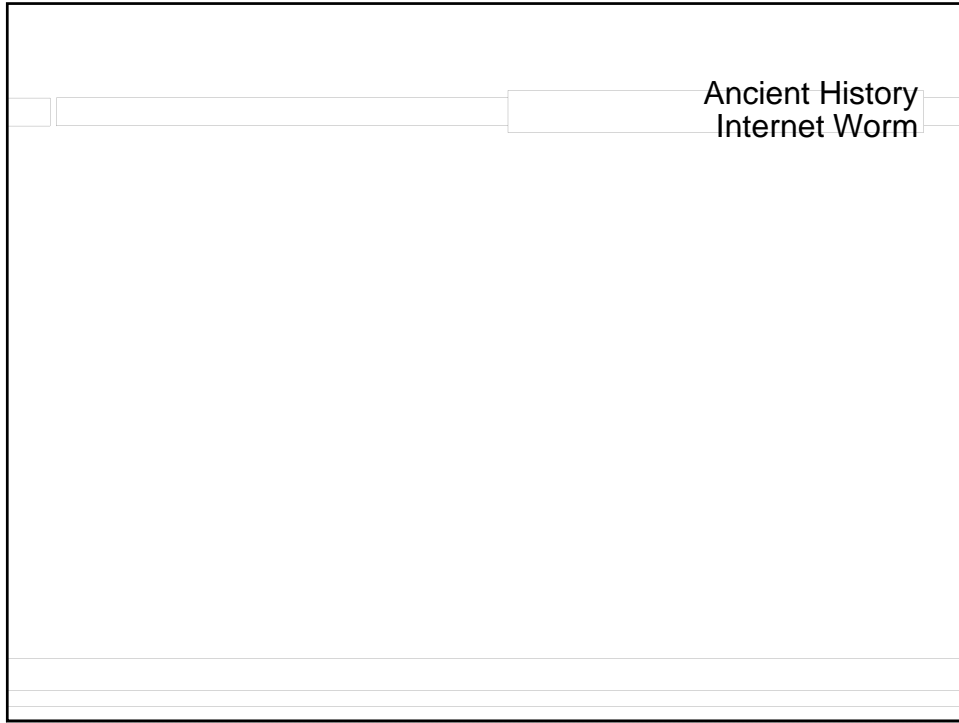


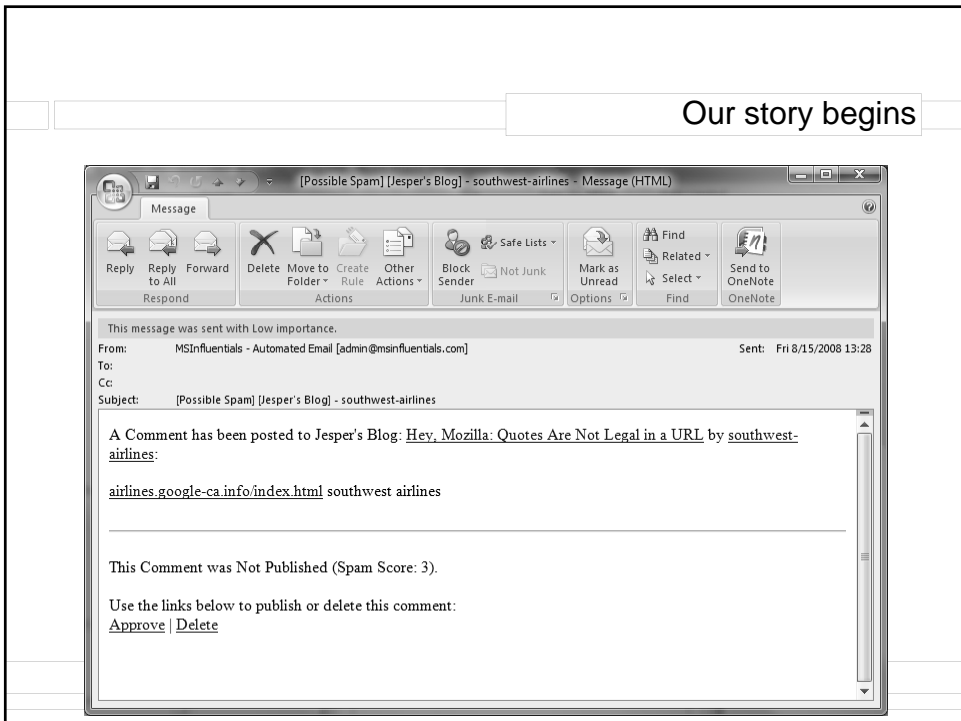
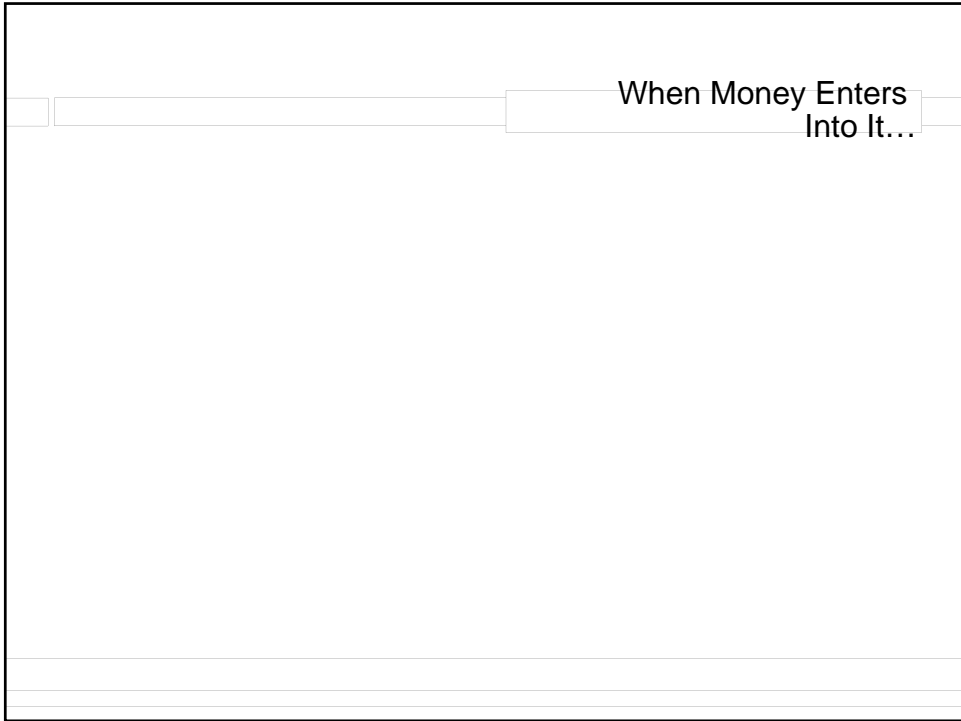
Anatomy of a Hack, 2008

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

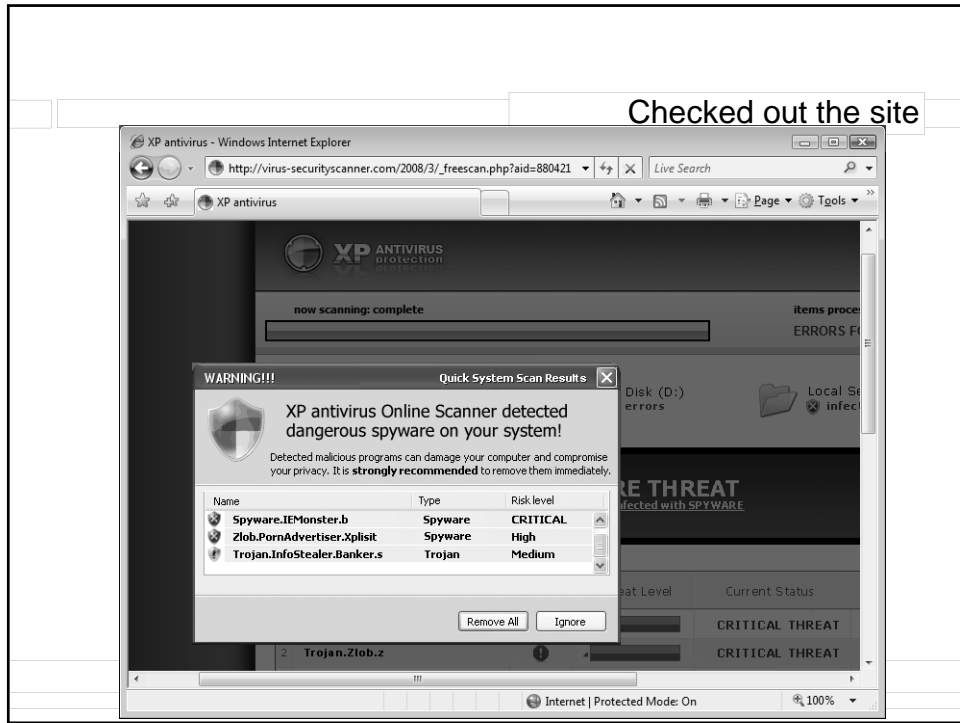
Key Takeaways

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



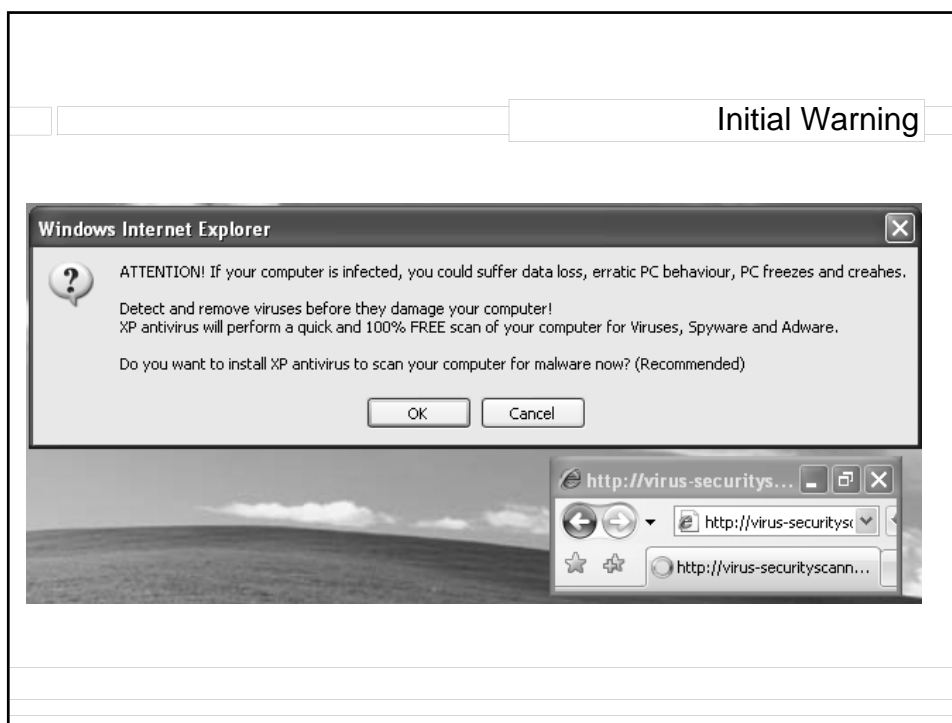


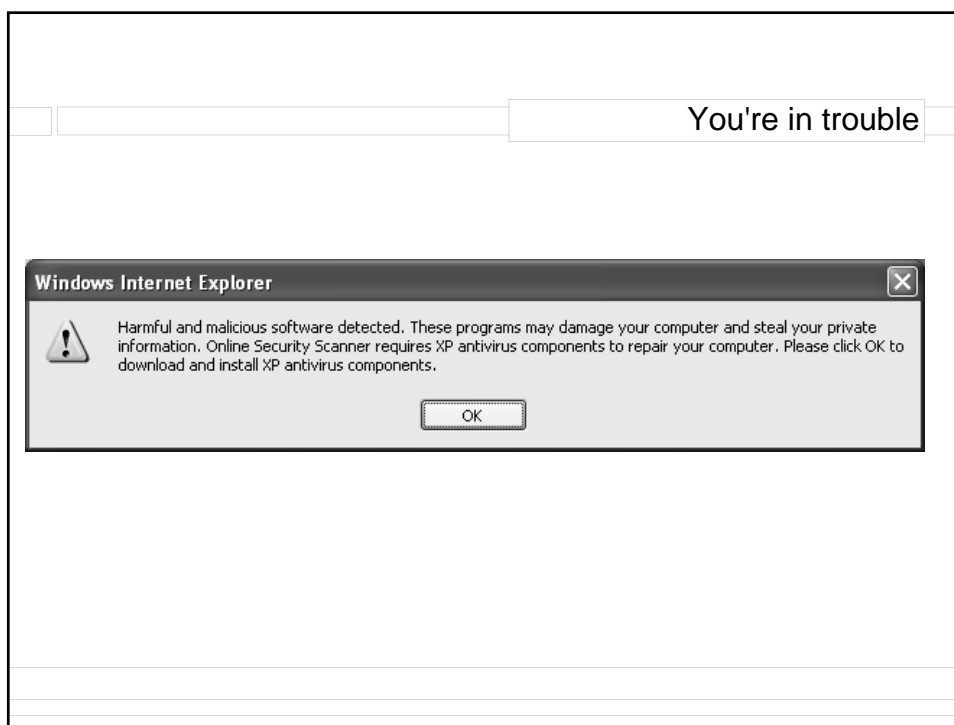
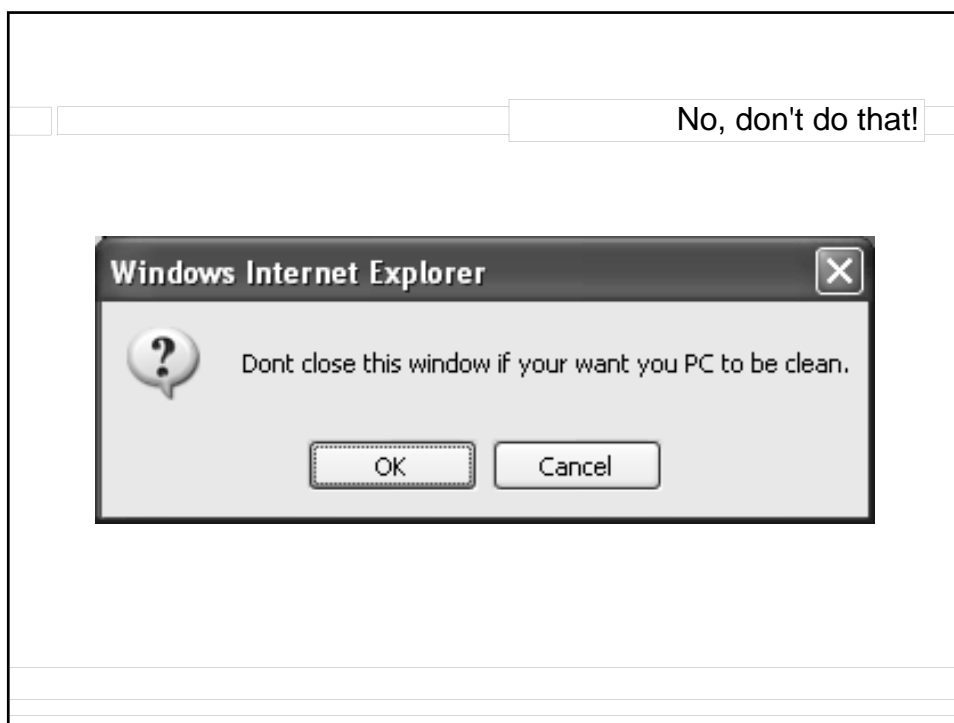
Checked out the site



Demo

THE MALICIOUS SITE

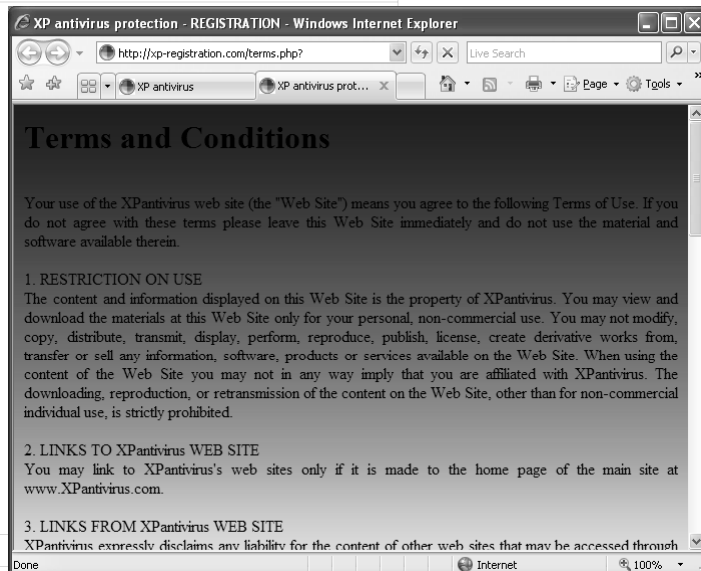




But we can help



Surrender and accept terms



ANTIVIRUS XP 2008 LICENSE AGREEMENT

First half of 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. IF YOU DO NOT ACCEPT THE TERMS AND CONDITIONS OF THIS AGREEMENT, IF YOU 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 agreement 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 release of Antivirus XP 2008. In case of a disk replacement, 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 for 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:

- 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 of Antivirus XP 2008;**
- C. use a previous version of Antivirus XP 2008 after You have received a disk replacement set or upgrade of 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;

Second half of license agreement

2. Refunds Policy

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. AntivirusXP2008.com is not responsible for any help the customer gets from third party software. The customer is responsible for 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 the customer before uninstalling such products. The customer is responsible for the installation or removal of such software.

Existence 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. Refunds will not be granted on the grounds of the Software not performing any function it was not created to perform. The issues the customer is responsible for are the interaction of the Software with other software.

AntivirusXP2008.com is not responsible for any harmful infections.

In this case, our customer department will analyze the customer's system data and reports 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 a few cases, a refund will be granted. A refund will be granted if the customer has purchased AntivirusXP2008.com is not responsible for the refund.

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 an alternative download method within 72 hours after the complaint was filed. Declaring a refund is NOT possible within the 72-hour 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.

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 the use of the Software will meet your requirements or that the Software will be uninterrupted or that Antivirus XP 2008 will be available for use in a specific environment. You assume the 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.com setup procedure may uninstall some products or some components in order to avoid their incompatibility with the Software. ANTIVIRUS XP 2008 automatically adds AntivirusXP2008.com sites to Internet Explorer trusted zone.

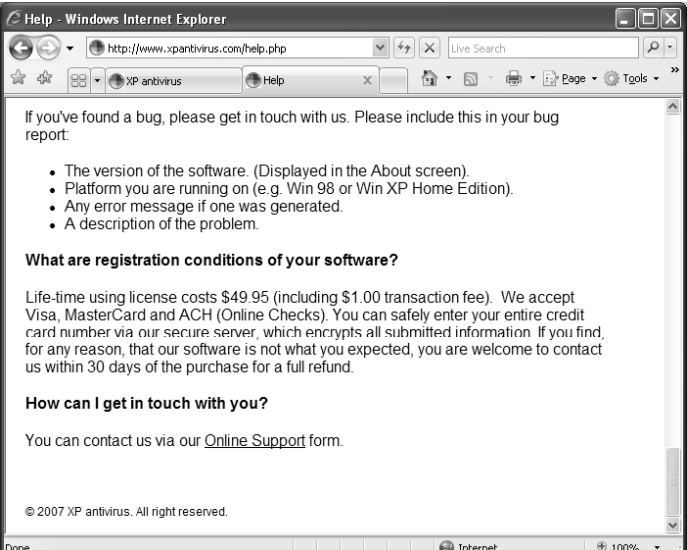
THE ABOVE WARRANTY IS EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER 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.

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



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?

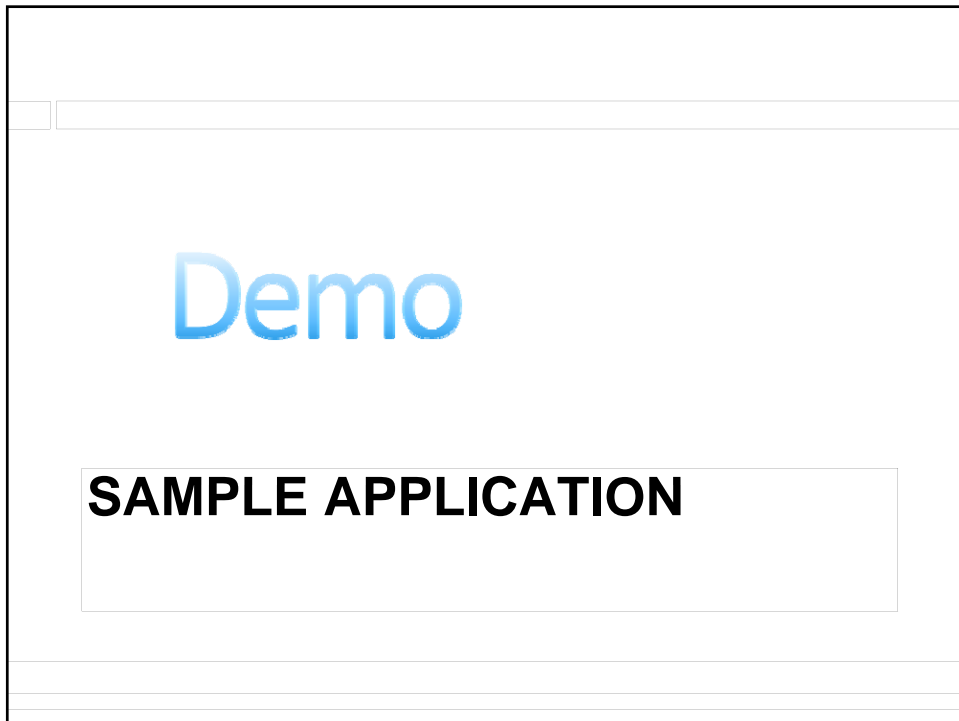
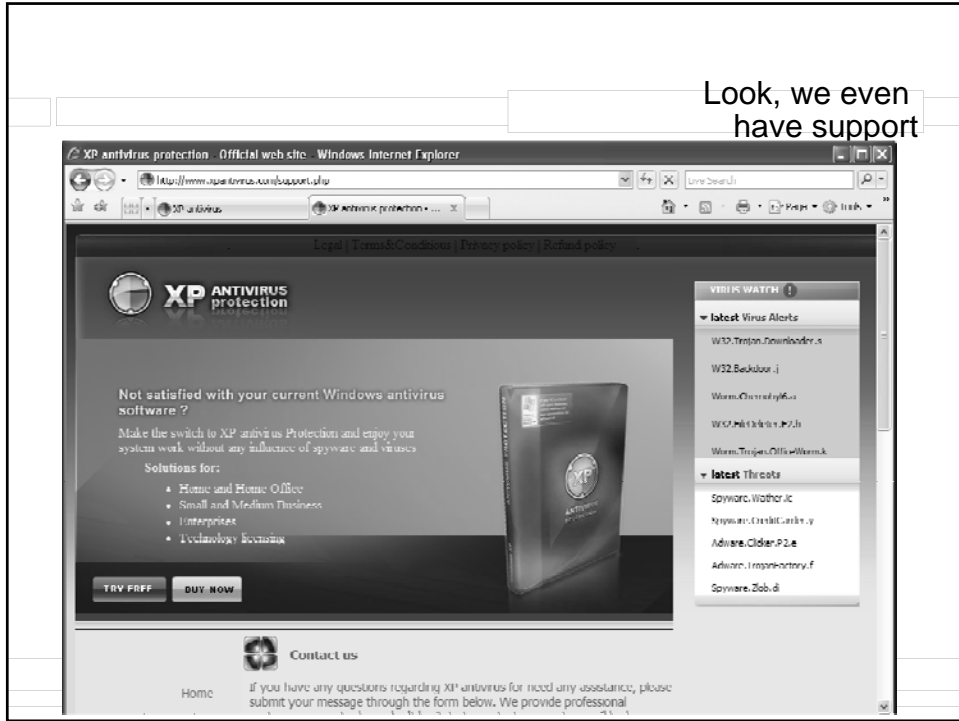
Life-time using license costs \$49.95 (including \$1.00 transaction fee). We accept Visa, MasterCard and ACH (Online Checks). You can safely enter your entire credit card number via our secure server, which encrypts all submitted information. If you find, for any reason, that our software is not what 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.

© 2007 XP antivirus. All right reserved.

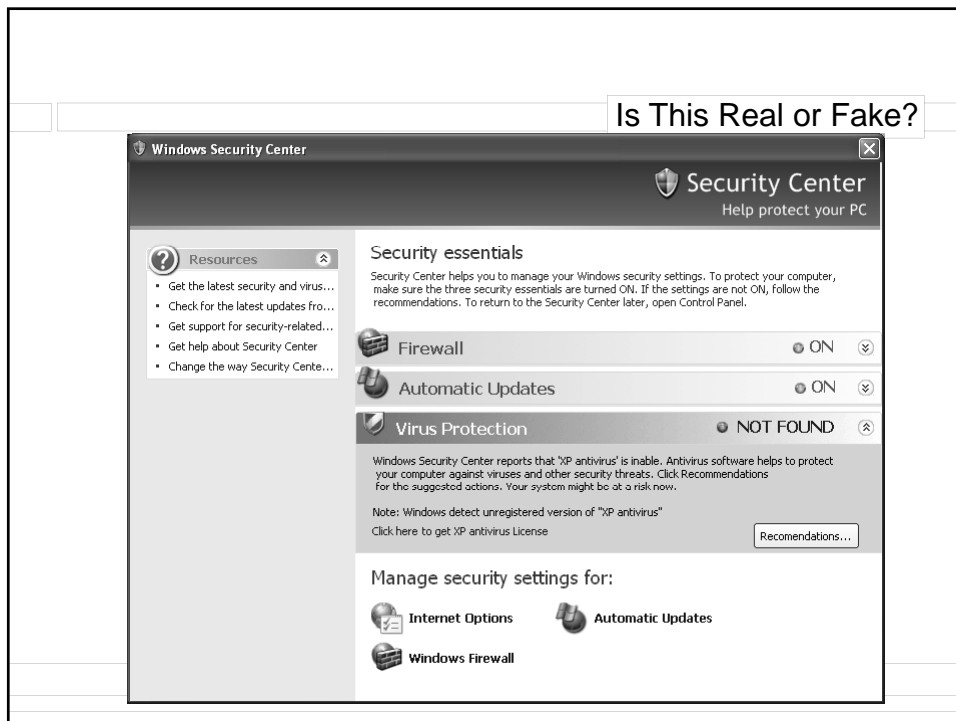
Look, we even have support

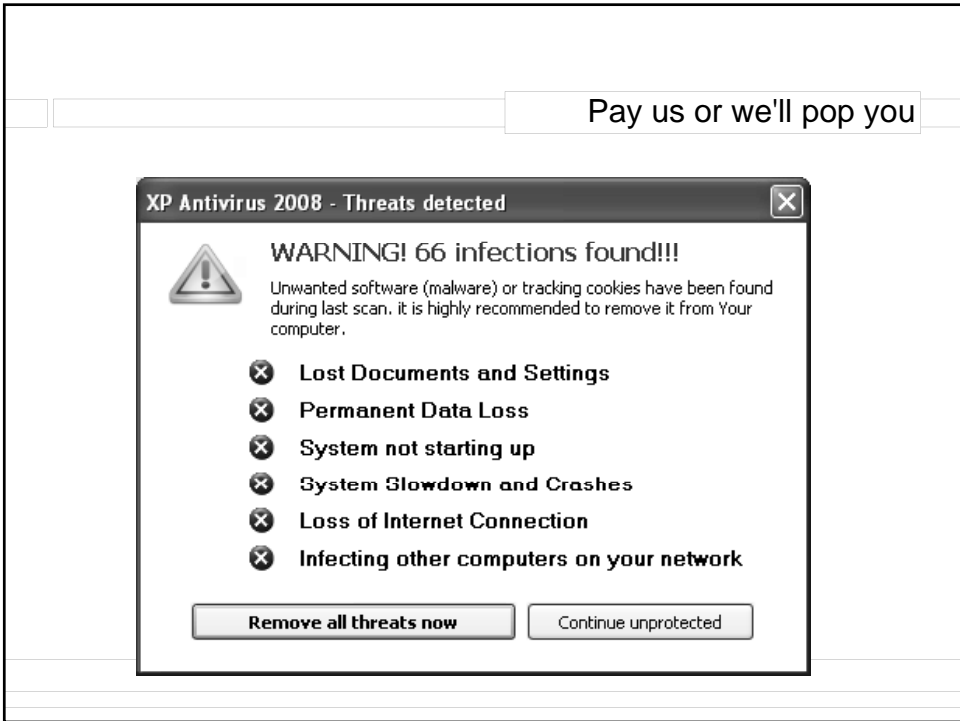
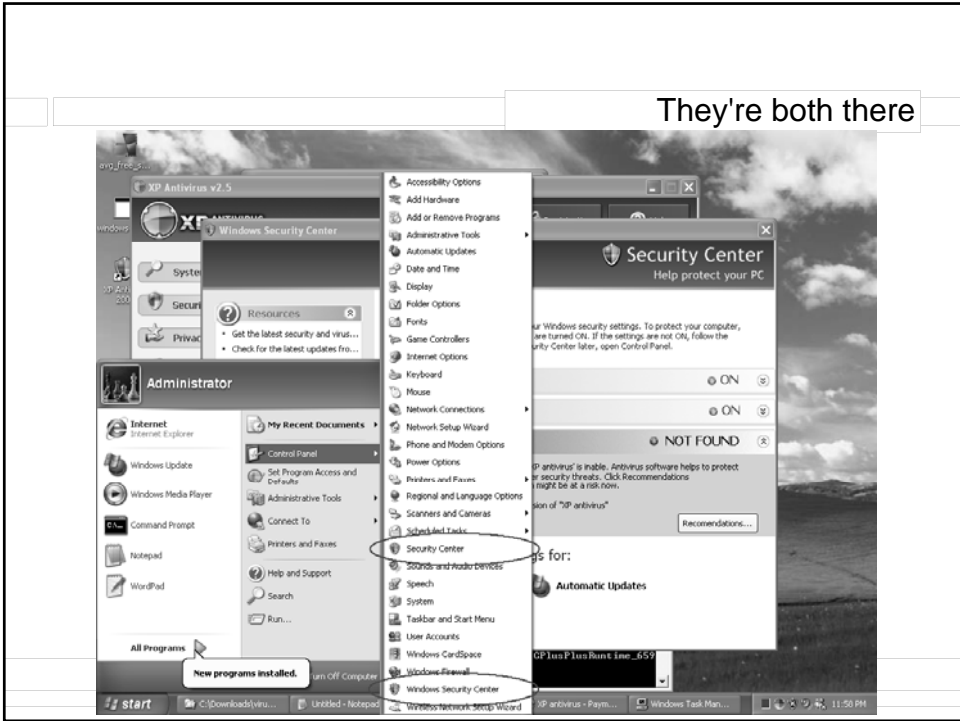


Is This Real or Fake?

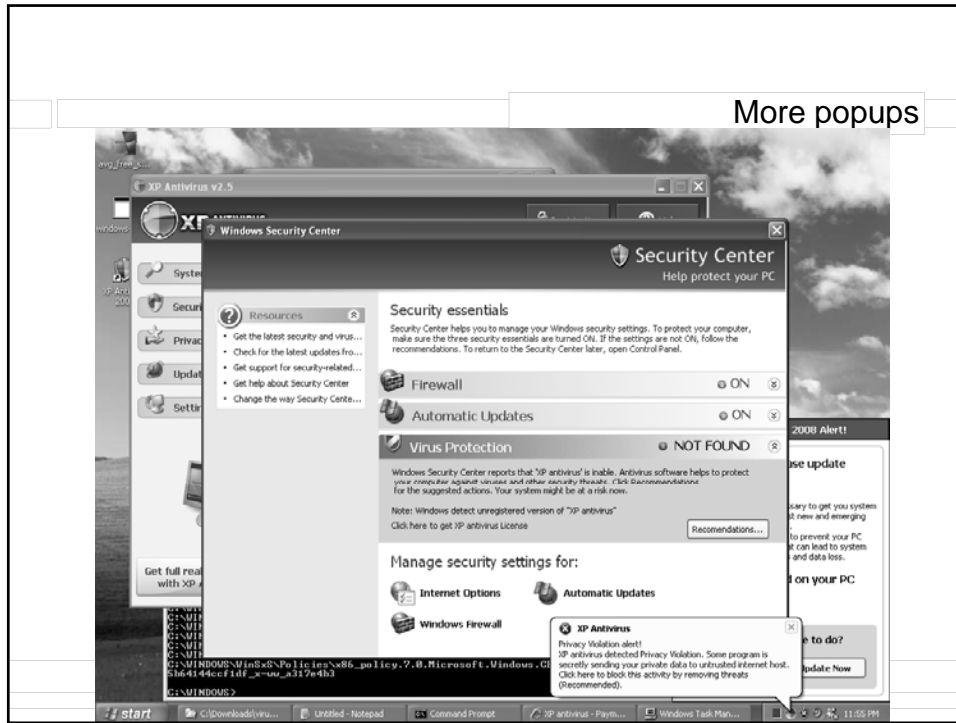


Is This Real or Fake?



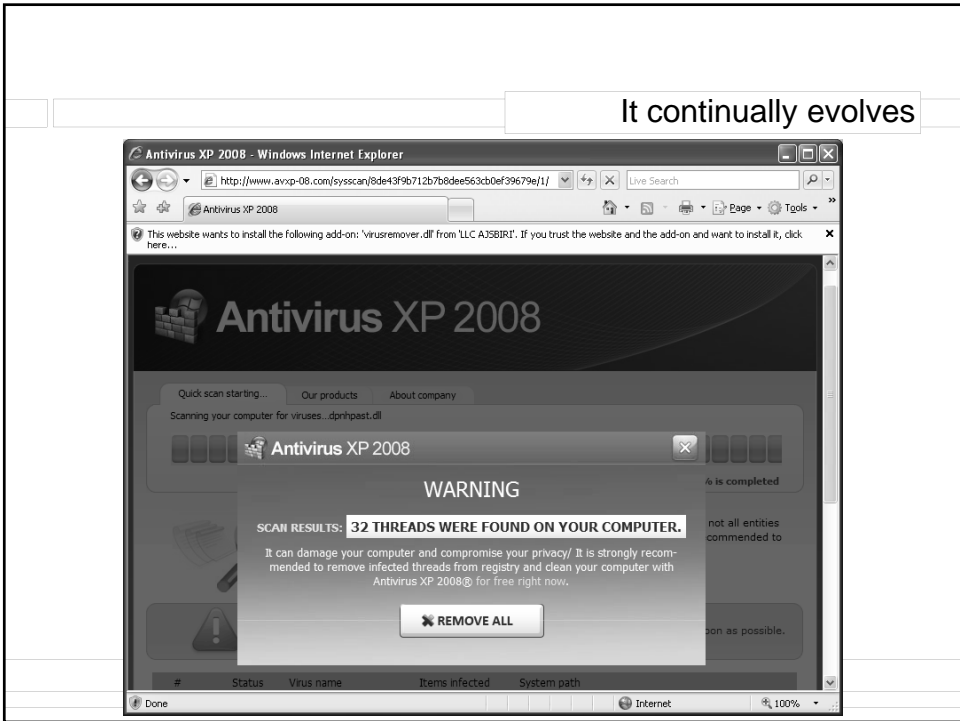
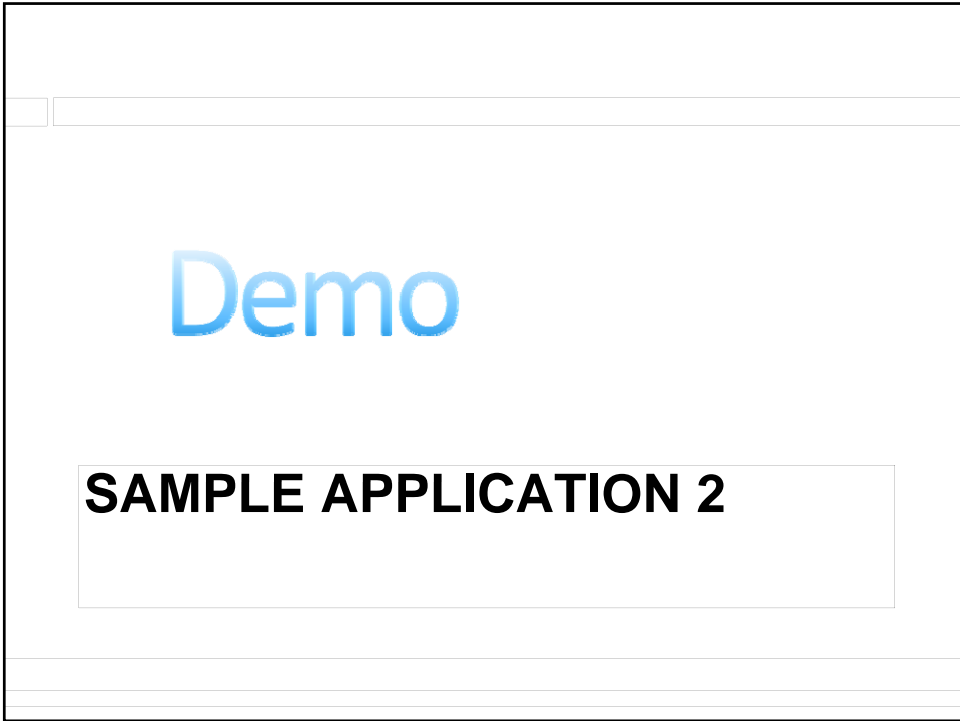


More popups

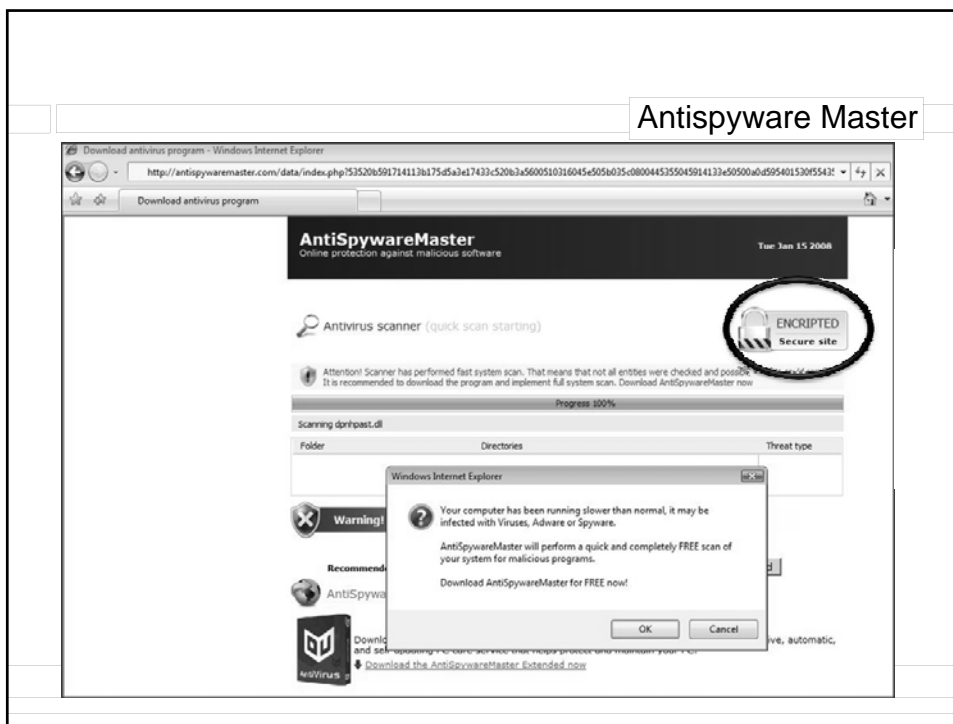


The app itself

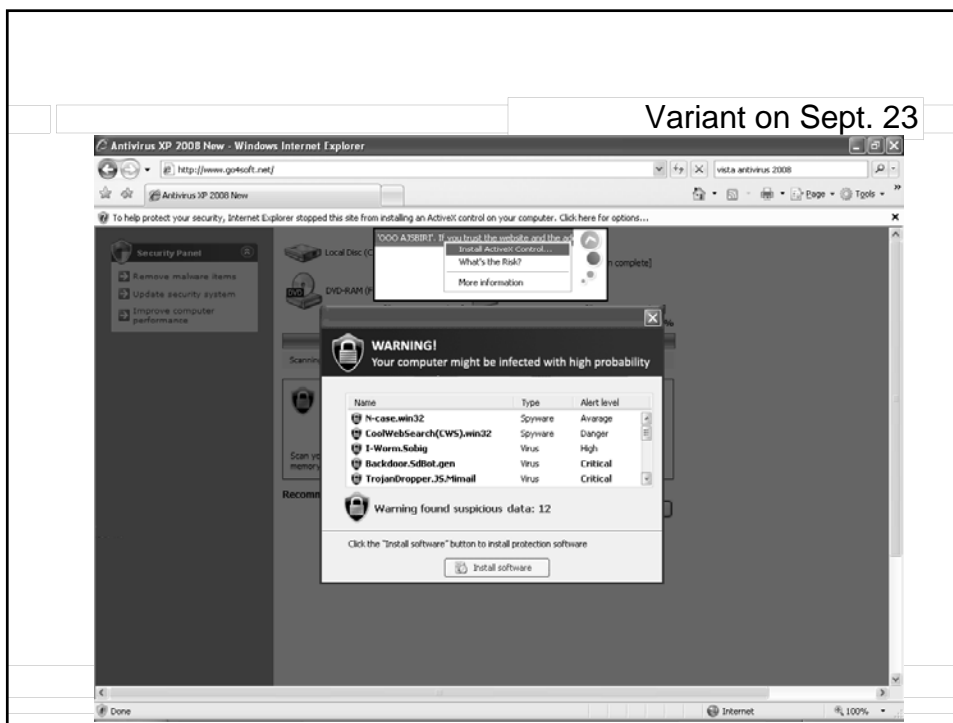




Antispyware Master



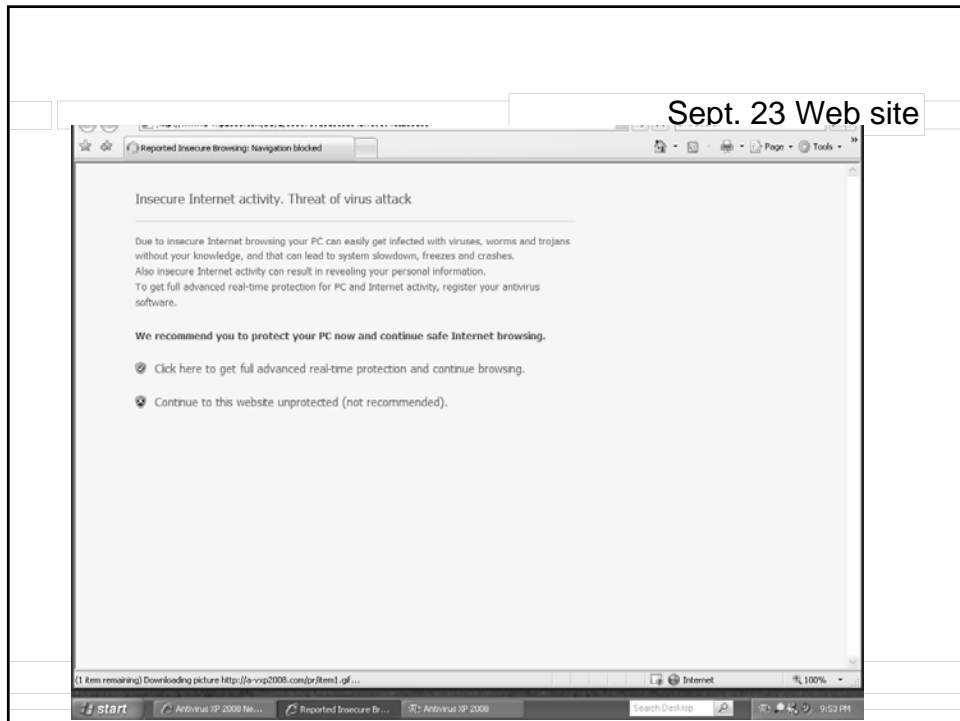
Variant on Sept. 23



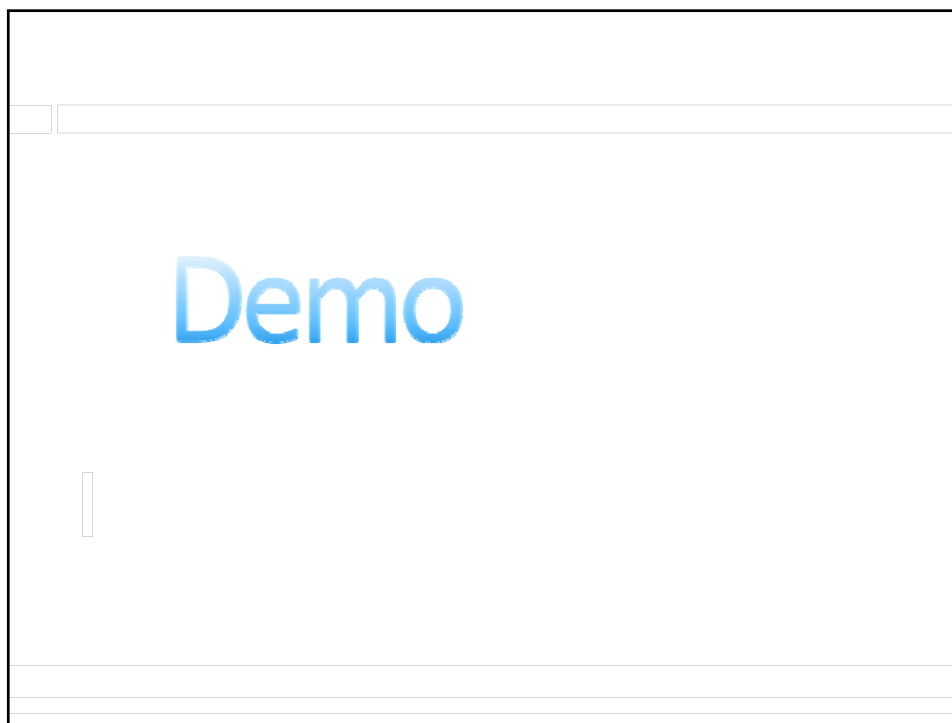
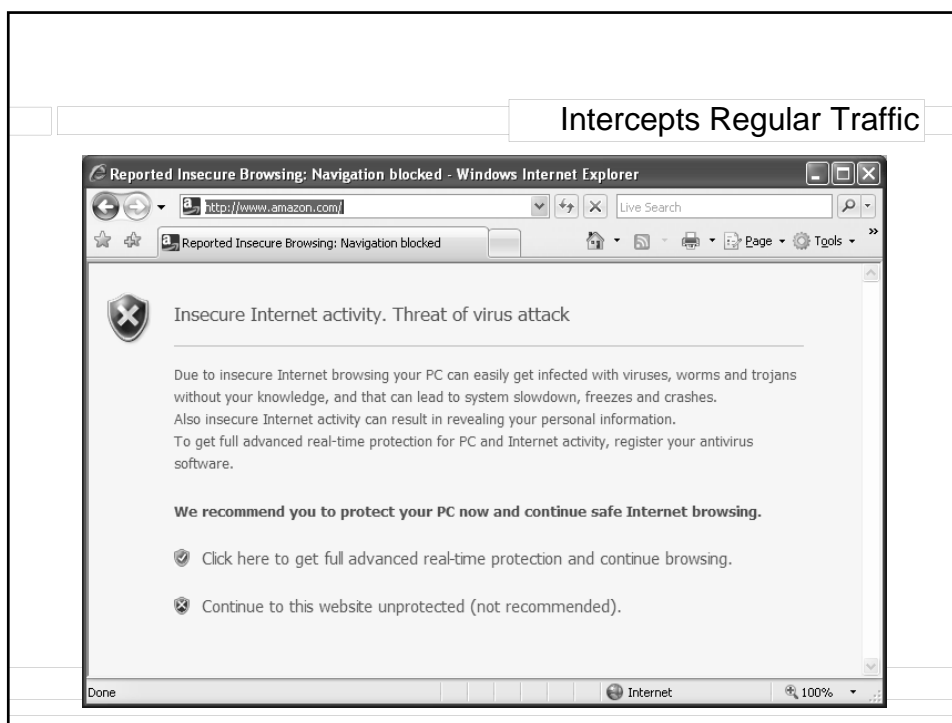
Sept. 23 software



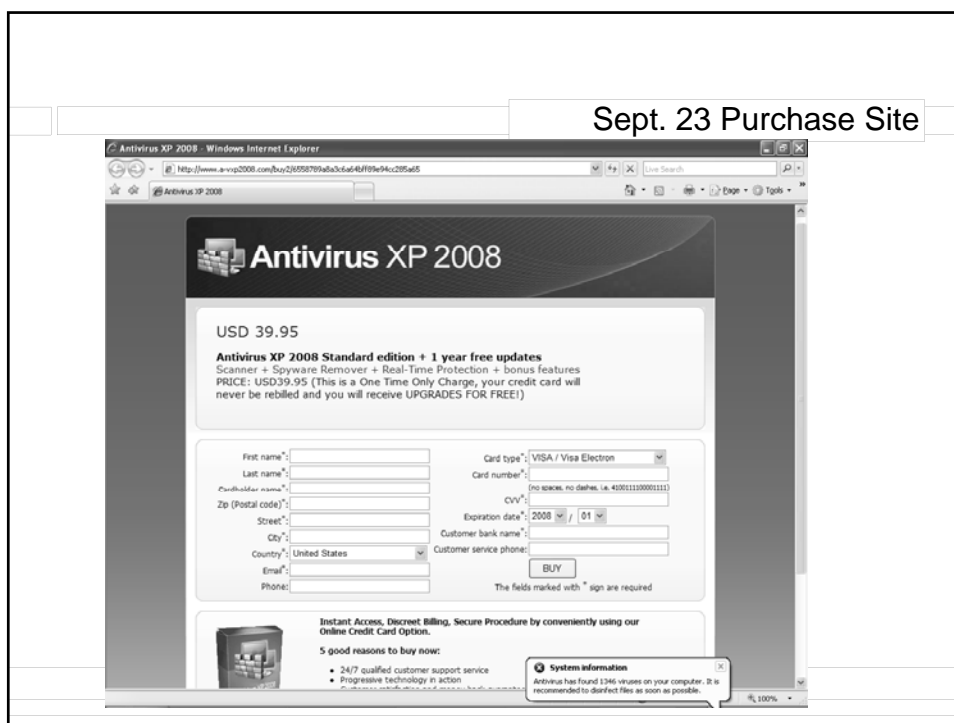
Sept. 23 Web site



Intercepts Regular Traffic



Sept. 23 Purchase Site



Charges

➤ **\$82.90** each from:

COUNTRY	DATE/TIME	MERCHANT NAME/CITY
RU	09/09 20:23	SPYWARE-SHOP2.CO
LV	09/09 20:23	WAV2008.COM RIGA
RU	09/09 20:27	WWW.SPYWARE-MALL
LV	09/09 20:28	WAV2008.COM RIGA
RU	09/09 20:27	SPYWARE-SHOP6.CO

Registration Information

```

Domain Name: a-vxp2008.com
Record created: 2008/9/16
Record expired: 2009/9/16

Domain servers in listed order:
ns1.a-vxp2008.com      ns3.a-vxp2008.com

Administrative:
name-- DNS MANAGER
org-- ABSOLUTE CORP. LTD.
country-- CN
province-- Hongkong
city-- Hongkong
address-- FLAT/RM 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
org-- ABSOLUTE CORP. LTD.
country-- CN
province-- Hongkong
city-- Hongkong
address-- FLAT/RM B 8/F CHONG MING BUILDING 72 CHEUNG SHA WAN RD KL
postalcode-- 999077
telephone-- +00.85223192933
fax-- +00.85223195168
E-mail-- a-3450400426302@absolute.com

Domain Name: GO4SOFT.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:
ns4.2ru.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

```

Tricks They Are Known To Be Using

- **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**