SOPHOS

What is FakeAV?

FakeAV or Fake AntiVirus, also known as Rogue AntiVirus, Rogues, or ScareWare, is a class of malware that displays false alert messages to the victim concerning threats that do not really exist. These alerts will prompt users to visit a website where they will be asked to pay for these non-existent threats to be cleaned up. The FakeAV will continue to send these annoying and intrusive alerts until a payment is made.

This paper provides insight into where FakeAV comes from, what happens when a system is infected with FakeAV, and how users can protect themselves from FakeAV.

A Sophos white paper

May 2010

What is FakeAV?

Introduction

FakeAV or Fake AntiVirus, also known as Rogue AntiVirus, Rogues, or ScareWare, is a class of malware that displays false alert messages to the victim concerning threats that do not really exist. These alerts will prompt users to visit a website where they will be asked to pay for these non-existent threats to be cleaned up. The FakeAV will continue to send these annoying and intrusive alerts until a payment is made.

This paper provides insight into where FakeAV comes from, what happens when a system is infected with FakeAV, and how users can protect themselves from FakeAV.

During the last year, the number of FakeAV executables has grown enormously. SophosLabs has seen the quantity of unique variants grow from less than 1,000 to well over half a million. This huge rise in popularity among malware writers is primarily due to the direct revenue source that FakeAV provides. Compared to other classes of malware such as bots, backdoor Trojans, downloaders and password stealers, FakeAV draws the victim into handing money over directly to the malware author. FakeAV is also associated with a thriving affiliate network community that makes large amounts of money by driving traffic toward the stores of their partners.[1]

Typical signs of infection

FakeAV usually uses a large array of social engineering techniques to get itself installed. Campaigns have included:

- Fake Windows Security Updates[2]
- Fake Virus-Total pages[3]
- Fake Facebook app[4]
- 9/11 scams[5]

Once on a system, there are many common themes in its behavior:

- **Popup warnings**
  Many FakeAV families will display popup messages in the taskbar:

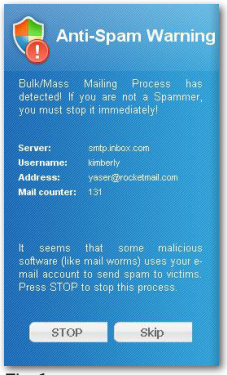


Fig.1

Fig.2

Fig.3

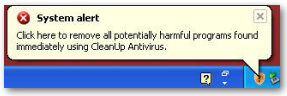


Fig.4

» **Fake scanning**
The FakeAV will typically pretend to scan the computer and find non-existent threats, sometimes creating files full of junk that will then be detected[6]:

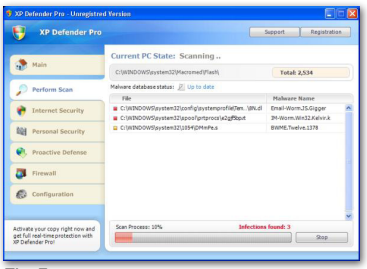


Fig.5

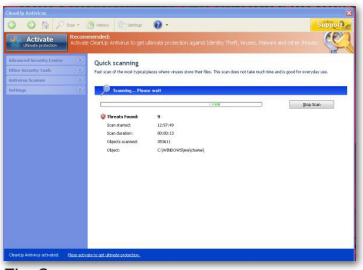


Fig.6

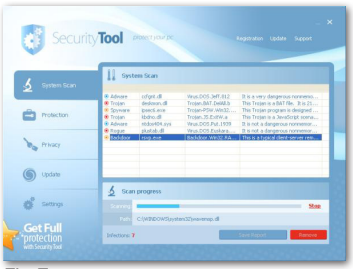


Fig.7

FakeAV uses an enormous range of convincing names to add to the illusion of legitimacy, such as:

» AntiSpyWarePro
» Antivirus Plus
» Antivirus Soft
» Antivirus XP
» Internet Security 2010
» Malware Defense
» Security Central
» Security Tool
» Winweb Security
» XP Antivirus
» Digital Protector
» XP Defender
» CleanUp AntiVirus

There can be many thousands of variants for each family as techniques such as server-side polymorphism are used heavily to alter the FakeAV executable. This is a process whereby the executable is re-packaged offline and a different file is delivered when a download request is made. This can happen many times during a 24-hour period. One particular family that calls itself “Security Tool”[7] has been known to produce a different file nearly every minute. This is how a single family can have such large numbers of samples.

Many families will also share a common code base underneath the polymorphic packer, where the application is simply “re-skinned” with a different look and feel but the behavior remains the same.

Infection vectors

How do people get infected with FakeAV?

Although there are many different ways that a specific FakeAV may get onto a system, the majority of distribution avenues rely on social engineering. Ultimately, the user is tricked into running the FakeAV installer executable in a way similar to many other types of Trojans. FakeAV authors have used a huge range of different social engineering tricks and are continuing to come up with new ones all the time.

In this paper, we review several main sources of FakeAV infection:

- Search engine optimization poisoning
- Email spam campaigns
- Compromised websites and exploit payloads
- FakeAV downloads by other malware

Search engine optimization poisoning

A very common source of FakeAV infection is following results received from popular search engines while searching for topical terms. FakeAV authors ensure that links leading to FakeAV download sites will feature prominently in search results by using blackhat SEO techniques.[8] These poisoned results will redirect users to a FakeAV-controlled website that displays a fake scanning page, informing them that their computer is infected and they must download a program to clean it up. Alternatively, a fake movie download page may be displayed, where users are prompted to download a codec in order to view the movie. This codec is in fact a FakeAV installer.

Google Trends[9] is a service provided by Google that highlights popular search terms entered into its search engine. Here is an example of how search terms taken from Google Trends are poisoned by FakeAV authors. Let's do a search over the last 24 hours for pages containing terms from Hot Searches:

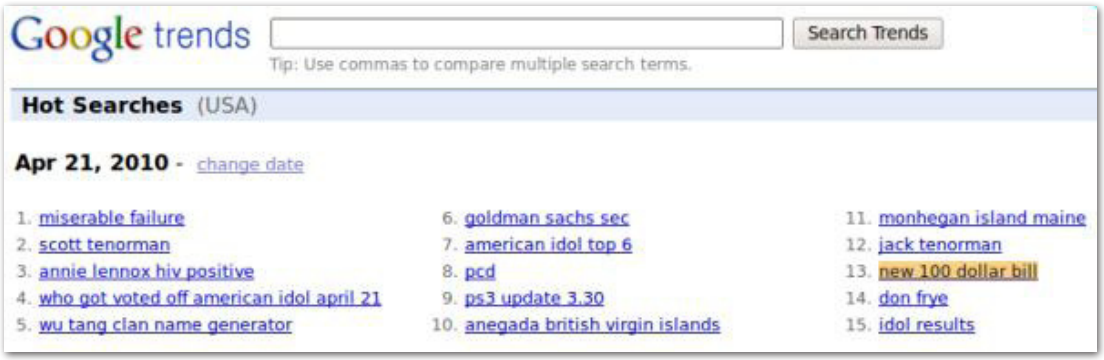


Fig.8

Picking several of the terms and performing a search for them will produce several poisoned results:

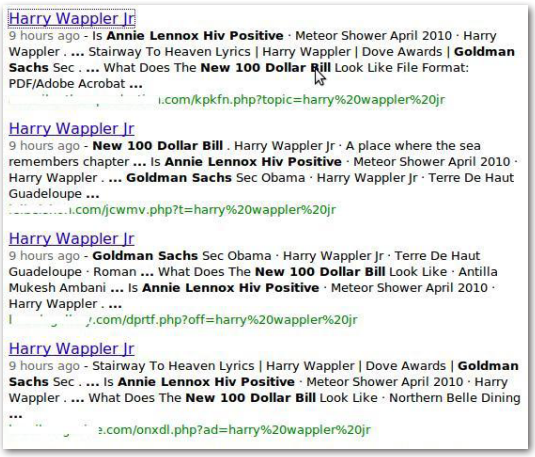


Fig.9

Clicking on these links takes users to a fake scanning page, where they are told they have multiple infections and need to download a program to remove the threats:

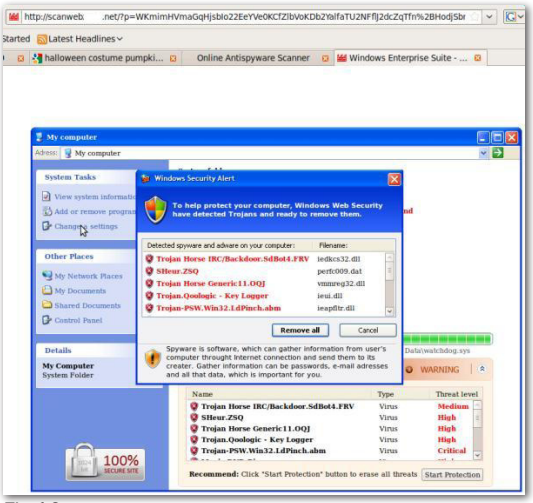


Fig.10

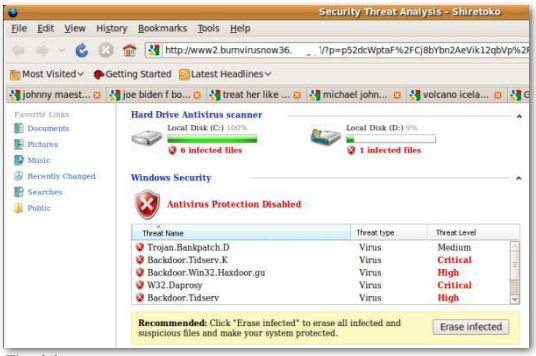


Fig.11

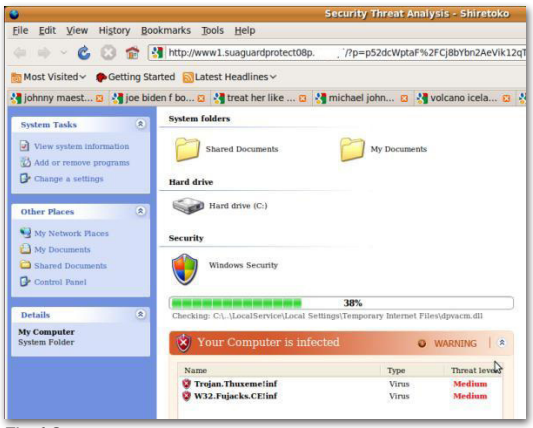


Fig.12

Or, users are taken to a fake movie download page where they are told they need to download a codec to view the movie:

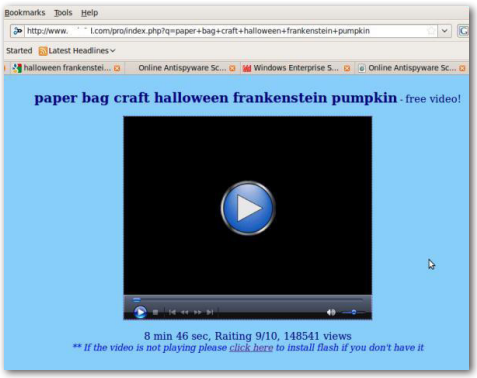


Fig.13

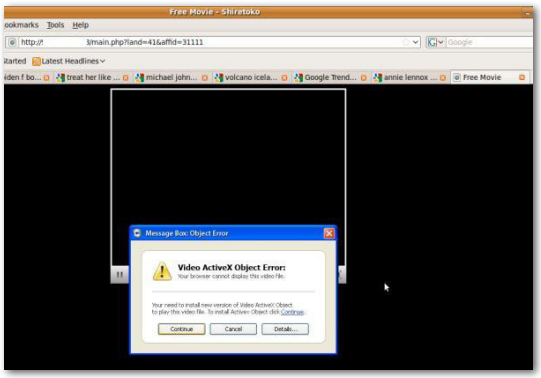


Fig.14

In each case, users are tricked into downloading and running an unknown executable, which is the FakeAV installer.

Spam campaigns

FakeAV is often sent directly to the victim as an attachment or as a link in a spam message. The message is predominantly sent through email, but other forms of spam have also been observed to deliver FakeAV, such as instant messaging applications including Google Talk.[10] The spam message itself usually uses social engineering techniques to trick users into running the attached file or clicking on the link. Specific campaigns vary and include password reset, failed delivery message and "You have received an ecard" scams.

Examples of email spam campaigns spreading FakeAV include:

» **Account suspension scams:** Victims receive an email message suggesting access to a specific account has been terminated and they need to run the attached file to fix the issue.

Fig.15

»

» **Ecard scams:** An email is received purporting to be from a legitimate ecard company. In fact, a FakeAV installer is attached.

Fig.16

» **Password reset scams:** Victims receive a message supposedly from a popular website, informing them that their password has been reset and the new one is in the attached file.

Fig.17

» **Package delivery scam:** Details of a (fictitious) recent postal delivery are included in an attached file. In reality, the attachment will install FakeAV.

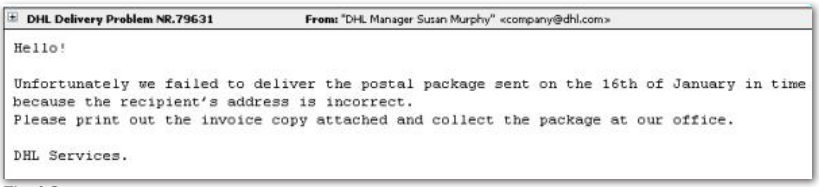


Fig.18

Compromised websites and exploit payloads

Users can sometimes be sent to FakeAV websites by browsing legitimate websites that have been compromised, where malicious code has been injected into the page. This can be achieved by penetrating the target website's hosting server and appending (typically) JavaScript to HTML pages hosted there. This redirect code can be used to send the browser to any type of malware hosting page including exploit kits and FakeAV. This JavaScript code is almost always heavily obfuscated, and Sophos detects this type of malware as variants of Troj/JSRedir.[11]

SophosLabs has also seen hackers compromise legitimate web-based advertising feeds to ensure that malicious code is loaded instead. This may take the form of an exploit that downloads and executes a FakeAV binary as the payload or a simple iframe that redirects the browser to a FakeAV web page.[12,13]

FakeAV downloads by other malware

FakeAV can be downloaded onto a machine by other types of malware. SophosLabs maintains many honeypot machines that are seeded with different malware, in order to observe their behavior and ensure protection is maintained when new variants are downloaded. We have seen several families install FakeAV onto an infected machine, most notably TDSS, Virtumundo and Waled.[14] The infamous Conficker worm was also observed to install FakeAV onto infected computers.[15] In this way, a hacker that has infected a computer with TDSS or Virtumundo can extract more money from victims by forcing them to pay for FakeAV.

FakeAV families

We now explain in more detail the behavior of FakeAV once it has made its way onto a target system.

Registry installation

FakeAV's typical behavior is to copy the installer to another location on the system and create a registry entry that will run the executable on system startup.

The installer is often copied into the user's profile area (e.g., C:\Documents and Settings\<user>\Local Settings\Application Data), or into the temporary files area (e.g., c:\windows\temp) with a randomly generated file name. This makes the FakeAV UAC-compliant on Windows machines that have UAC[16] enabled, thus avoiding a UAC warning popping up during installation. However, some families still do not care about UAC and still create their files in the Program Files or Windows folders.

A run key entry is then created in the registry that will run the file when the system starts up. Typically, this will be added to one of the following:

- HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce
- HKCU\Software\Microsoft\Windows\CurrentVersion\Run
- HKLM\Software\Microsoft\Windows\CurrentVersion\Run

Examples:

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
wpkarufv

c:\documents and settings\<user>\local settings\application data\tqaxywicl\chgutertssd.exe

HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce
CUA

c:\windows\temp\sample.exe

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
85357230

c:\documents and settings\all users\application data\85357230\85357230.exe

Initiate a fake scan

Once FakeAV is installed, it will usually attempt to contact a remote website over HTTP and will often download the main component. This will initiate a fake system scan, where many non-existent threats will be discovered. The main FakeAV window is often very professionally created and victims can easily be convinced that they are using a genuine security product. Here are several examples:

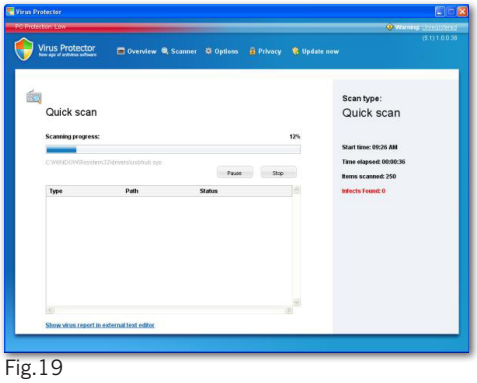


Fig.19

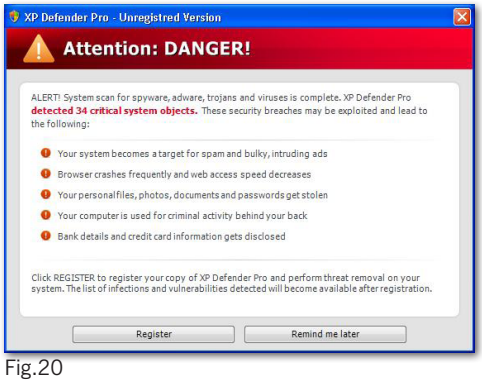


Fig.20

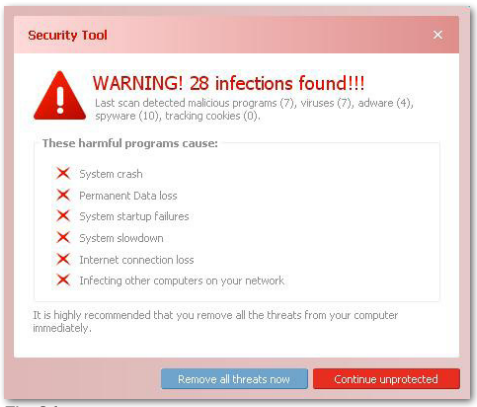


Fig.21

Fig.22

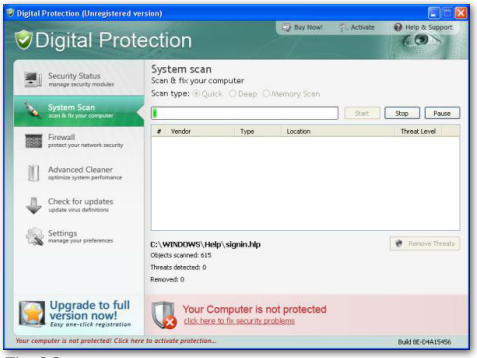


Fig.23

Once the fake threats have been discovered, users are told they must register or activate the product in order to clean up the threats. Users are taken to a registration website (either through a browser or through the FakeAV application), where they are asked to enter their credit card number and other registration details. These pages are also very convincing, occasionally featuring illegal use of logos and trademarks from industry-recognized organizations such as Virus Bulletin[17] and West Coast Labs[18]:

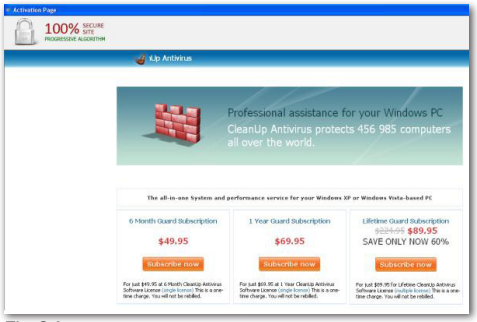


Fig.24

This example fraudulently uses logos from West Coast Labs and Virus Bulletin:

Fig.25

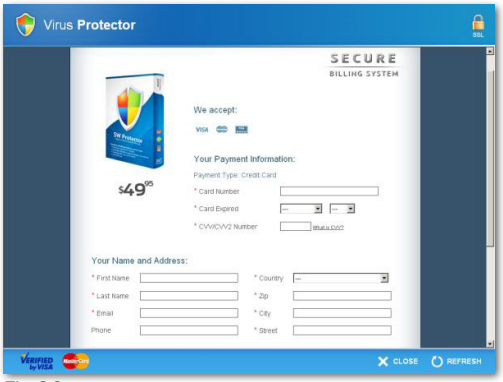


Fig.26

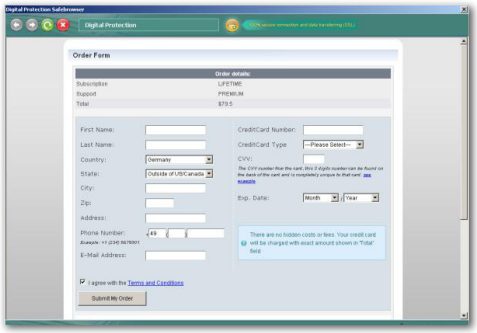


Fig.27

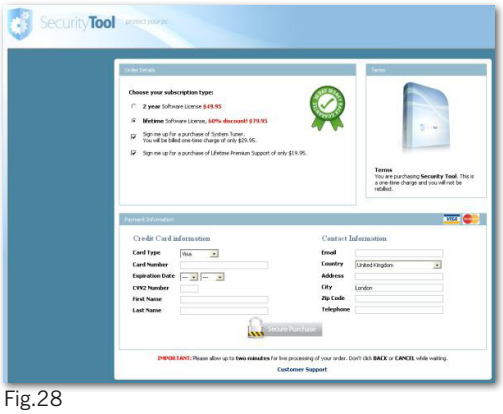


Fig.28

Other FakeAV behavior

Certain FakeAV families cause further distress to the victim by interfering with normal system activity. Commonly, this includes disabling the Task Manager and use of the Registry Editor, prohibiting certain processes from running and even redirecting web requests. This behavior further convinces the user that there is a problem on the system and increases the likelihood of a purchase being made. This extra activity can take the form of:

» **Process termination:** Certain programs are prohibited from running by the FakeAV, with a warning message being displayed instead.

Fig.29

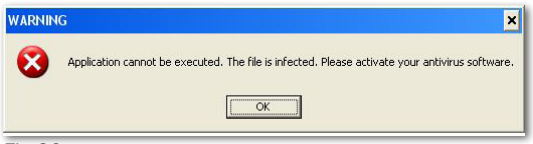


Fig.30

The FakeAV will generally allow Explorer and Internet Explorer to run, so renaming an executable as explorer.exe or iexplore.exe should allow it to be run.

» **Web page redirection:** Some FakeAV families will redirect web requests for legitimate web sites to an error message or other type of warning message. This adds to the user's fear and, again, makes the user more likely to pay for the FakeAV.

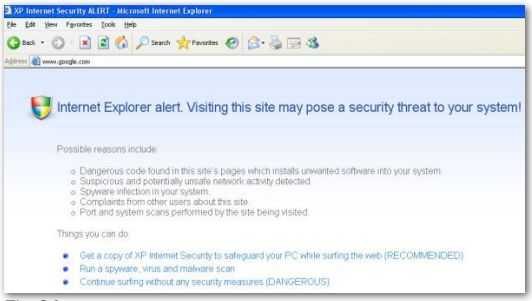


Fig.31

» **Installation of more malware:** FakeAV has been known to download other types of malware upon installation, such as banking Trojans, rootkits and spam bots.

Prevention and protection

The most effective defense against the FakeAV threat is a comprehensive, layered security solution. Detection can and should take place at each stage of the infection:

- **URL filtering:** By blocking the domains and URLs from which FakeAV is downloaded, the infection can be prevented from ever happening. Sophos customers are protected by URL filtering in Sophos Web Security and Control[19] and the latest endpoint security product.
- **Detection of web-based content:** This includes detection of the JavaScript and HTML used on FakeAV and fake codec web pages. Detection at this layer prevents the FakeAV binary from being downloaded (e.g., Mal/FakeAvJs, Mal/VidHtml).
- **Proactive detection of the FakeAV binary:** Using Behavioral Genotype technology, many thousands of FakeAV binaries can be detected with a single identity. The number of samples currently detected as variants of Mal/FakeAV and Mal/FakeAle is well in excess of half a million.
- **Run-time detection: I**f a FakeAV executable manages to evade the other layers of protection, Sophos's Host Intrusion Prevention System (HIPS) can detect and block the behavior of the FakeAV sample when it tries to execute on the system.[20] HIPS includes rules that specifically target FakeAV.
- **Spam blocking:** Sophos Email Security and Data Protection blocks spam containing FakeAV before a user even sees it.[21]

Conclusion

FakeAV is a prevalent and rapidly growing threat. The direct financial benefit gained from FakeAV means that it will not go away; in fact, it will likely become even more widespread.

FakeAV is already distributed through a large number of sources. The variety and inventiveness of its distribution will only increase.

Fortunately, users can protect themselves through a comprehensive and layered security solution that detects and defends against FakeAV at every possible level.

References

1 **"The Partnerka – What is it, and why should you care?"**
Sophos technical paper, http://www.sophos.com/security/technical-papers/samosseiko-vb2009-paper.html

2 **"FakeAV Uses False 'Microsoft Security Updates'"**
SophosLabs blog, http://www.sophos.com/blogs/sophoslabs/?p=8564

3 **"Free FakeAV at Virus-Total (That's not VirusTotal)"**
SophosLabs blog, http://www.sophos.com/blogs/sophoslabs/?p=8885

4 **"Phantom app risk used to bait scareware trap"**
The Register, http://www.theregister.co.uk/2010/01/27/facebook_scareware_scam

5 **"Scareware scammers exploit 9/11"**
Sophos blog, http://www.sophos.com/blogs/gc/g/2009/09/11/scareware-scammers-exploit-911

6 **"FakeAV Generates Own Fake Malware"**
SophosLabs blog, http://www.sophos.com/blogs/sophoslabs/?p=6377

7 **"Mal/FakeVirPk-A"**
Sophos security analysis, http://www.sophos.com/security/analyses/viruses-and-spyware/malfakevirpka.html

8 **"Poisoned search results: How hackers have automated search engine poisoning attacks to distribute malware"**
SophosLabs technical paper, http://www.sophos.com/sophos/docs/eng/papers/sophos-seo-insights.pdf

9 **Google Trends**
http://www.google.com/trends

10 **"Google Talk used to distribute Fake AV"**
Sophos blog, http://www.sophos.com/blogs/chetw/g/2010/03/20/google-talk-distribute-fake-av/

11 **"More fake AV SEO poisoning"**
SophosLabs blog, http://www.sophos.com/blogs/sophoslabs/?p=6765

12 **"New York Times pwned to serve scareware pop-ups"**
The Register, http://www.theregister.co.uk/2009/09/14/nyt_scareware_ad_hack/

13 **"Scareware Traversing the World via a Web App Exploit"**
SANS Institute InfoSec Reading Room, http://www.sans.org/reading_room/whitepapers/incident/scareware-traversing-world-web-app-exploit_33333

14 **"Mal/TDSS-A"**
Sophos security analysis, http://www.sophos.com/security/analyses/viruses-and-spyware/maltdssa.html
"Troj/Virtum-Gen"
Sophos security analysis, http://www.sophos.com/security/analyses/viruses-and-spyware/trojvirtumgen.html
"Mal/WaledPak-A"
Sophos security analysis, http://www.sophos.com/security/analyses/viruses-and-spyware/malwaledpaka.html

15 **"Conficker zombies celebrate 'activation' anniversary"**
The Register, http://www.theregister.co.uk/2010/04/01/conficker_anniversary/

16 **"User Account Control Step-by-Step Guide"**
Microsoft TechNet, http://technet.microsoft.com/en-us/library/cc709691(WS.10).aspx

17 **Virus Bulletin**
http://www.virusbtn.com/

18 **West Coast Labs**
http://www.westcoastlabs.com/

19 **Sophos Web Security and Control**
http://www.sophos.com/products/enterprise/web/security-and-control/

20 **Sophos HIPS**
http://www.sophos.com/security/sophoslabs/sophos-hips/index.html

21 **Sophos Email Security and Data Protection**
http://www.sophos.com/products/enterprise/email/security-and-control/

Screenshot appendix

Fig.1

Fig.2

Fig.3

Fig.4


Anti-Spam Warning
Bulk/Mass Mailing Process has detected! If you are not a Spammer, you must stop it immediately!
Server: smtp.inbox.com
Username: kimberly
Address: yaser@rocketmail.com
Mail counter: 131
It seems that some malicious software (like mail worms) uses your e-mail account to send spam to victims. Press STOP to stop this process.
STOP
Skip

Fig.5

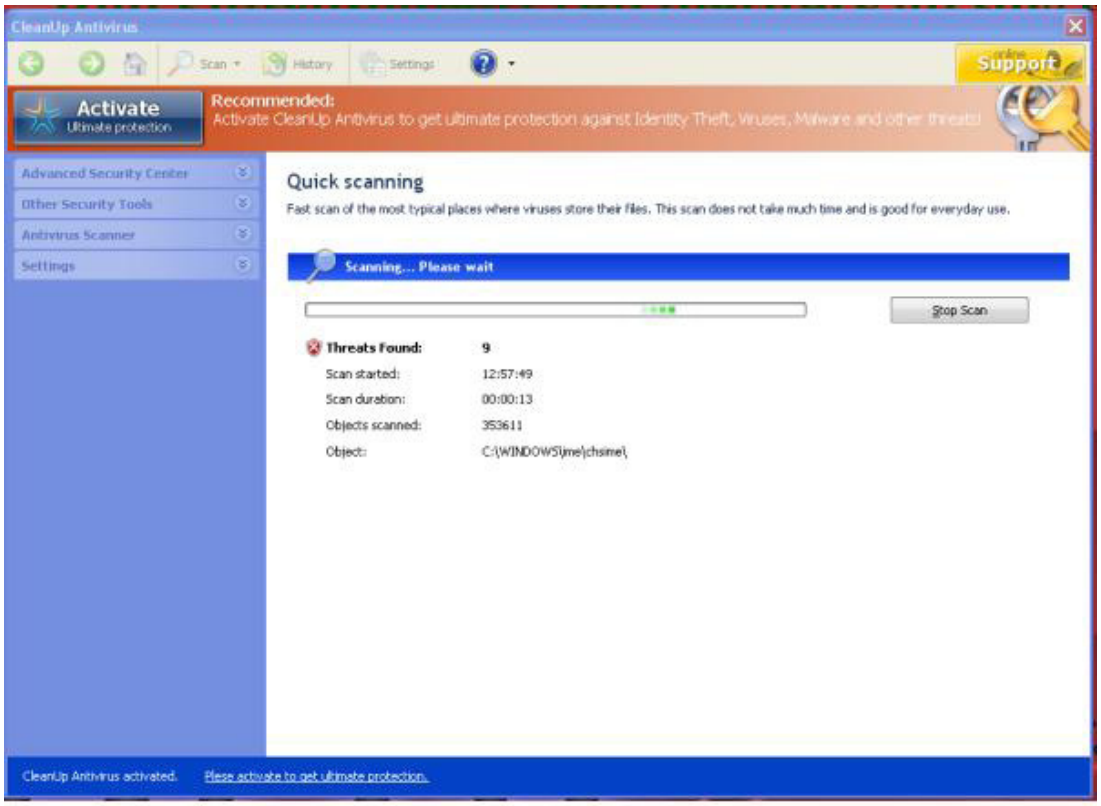

CleanUp Antivirus
Scan
History
Settings
Support
Activate
Ultimate protection
Recommended:
Activate CleanUp Antivirus to get ultimate protection against Identity Theft, Viruses, Malware and other threats!
Advanced Security Center
Other Security Tools
Antivirus Scanner
Settings
Quick scanning
Fast scan of the most typical places where viruses store their files. This scan does not take much time and is good for everyday use.
Scanning... Please wait
Stop Scan
Threats found: 9
Scan started: 12:57:49
Scan duration: 00:00:13
Objects scanned: 353611
Object: C:\WINDOWS\jme\chsime\
CleanUp Antivirus activated.
Please activate to get ultimate protection.

Fig.6

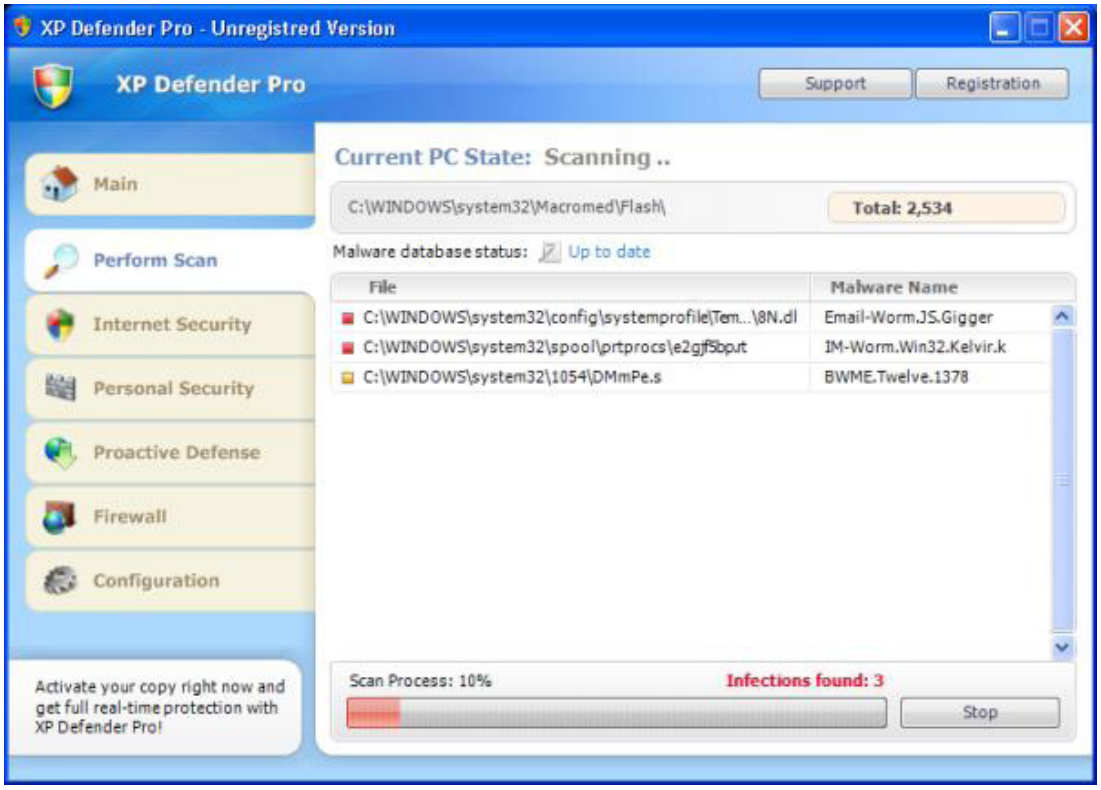

XP Defender Pro - Unregistred Version
XP Defender Pro
Support
Registration
Main
Perform Scan
Internet Security
Personal Security
Proactive Defense
Firewall
Configuration
Activate your copy right now and get full real-time protection with XP Defender Pro!
Current PC State: Scanning ..
C:\WINDOWS\system32\Macromed\Flash\
Total: 2,534
Malware database status: Up to date
File
Malware Name
C:\WINDOWS\system32\config\systemprofile\Tem...\8N.dl
Email-Worm.JS.Gigger
C:\WINDOWS\system32\spool\prtprocs\e2gjf5bput
IM-Worm.Win32.Kelvir.k
C:\WINDOWS\system32\1054\DMmPe.s
BWME.Twelve.1378
Scan Process: 10%
Infections found: 3
Stop

Fig.7

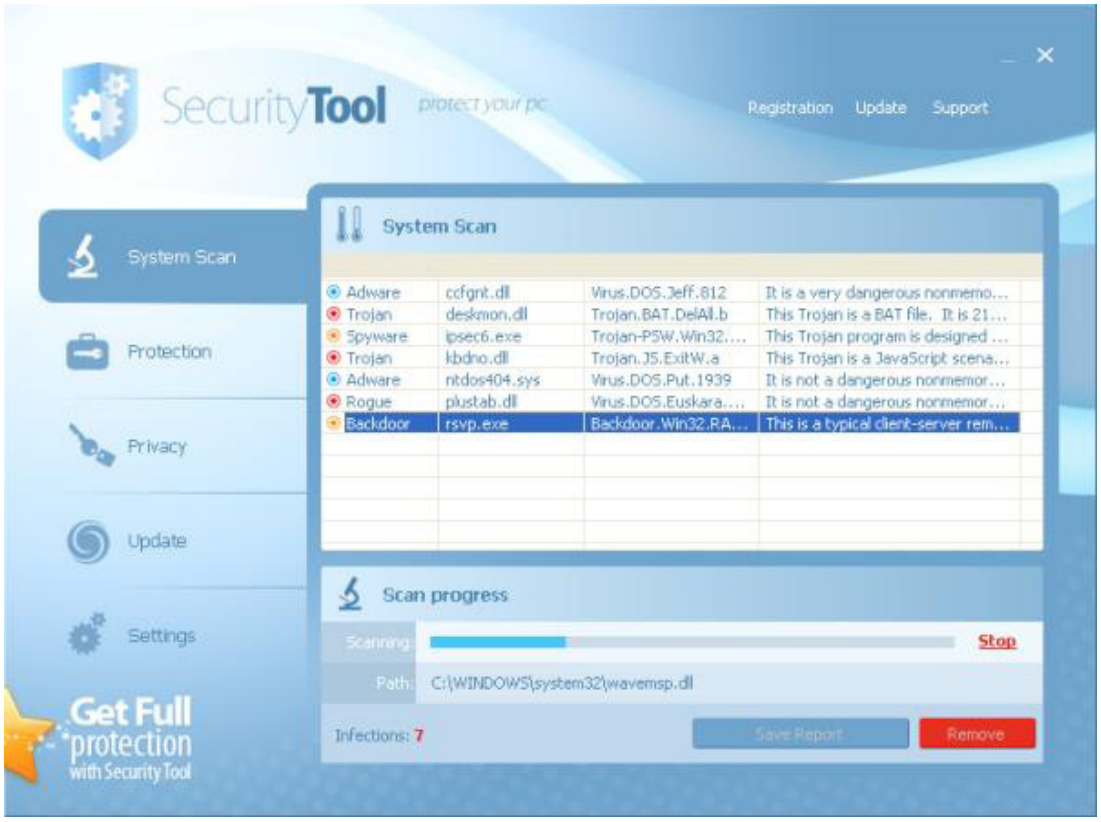

SecurityTool
protect your pc
Registration
Update
Support
System Scan
Protection
Privacy
Update
Settings
Get Full protection with Security Tool
System Scan
Adware ccfgnt.dll Virus.DOS.Jeff.812 It is a very dangerous nonmemo...
Trojan deskmon.dll Trojan.BAT.DelAll.b This Trojan is a BAT file. It is 21...
Spyware ipsec6.exe Trojan-PSW.Win32.... This Trojan program is designed ...
Trojan kbdno.dll Trojan.JS.ExitW.a This Trojan is a JavaScript scena...
Adware ntdos404.sys Virus.DOS.Put.1939 It is not a dangerous nonmemor...
Rogue plustab.dll Virus.DOS.Euskara.... It is not a dangerous nonmemor...
Backdoor rsvp.exe Backdoor.Win32.RA... This is a typical client-server rem...
Scan progress
Scanning:
Stop
Path: C:\WINDOWS\system32\wavemsp.dll
Infections: 7
Save Report
Remove

Fig.8

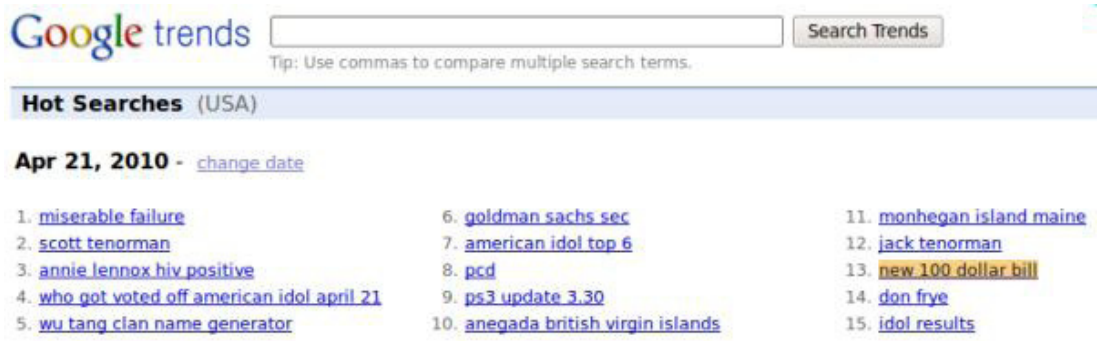

Google trends
Search Trends
Tip: Use commas to compare multiple search terms.
Hot Searches (USA)
Apr 21, 2010 - change date
1. miserable failure
2. scott tenorman
3. annie lennox hiv positive
4. who got voted off american idol april 21
5. wu tang clan name generator
6. goldman sachs sec
7. american idol top 6
8. pcd
9. ps3 update 3.30
10. anegada british virgin islands
11. monhegan island maine
12. jack tenorman
13. new 100 dollar bill
14. don frye
15. idol results

Fig.9

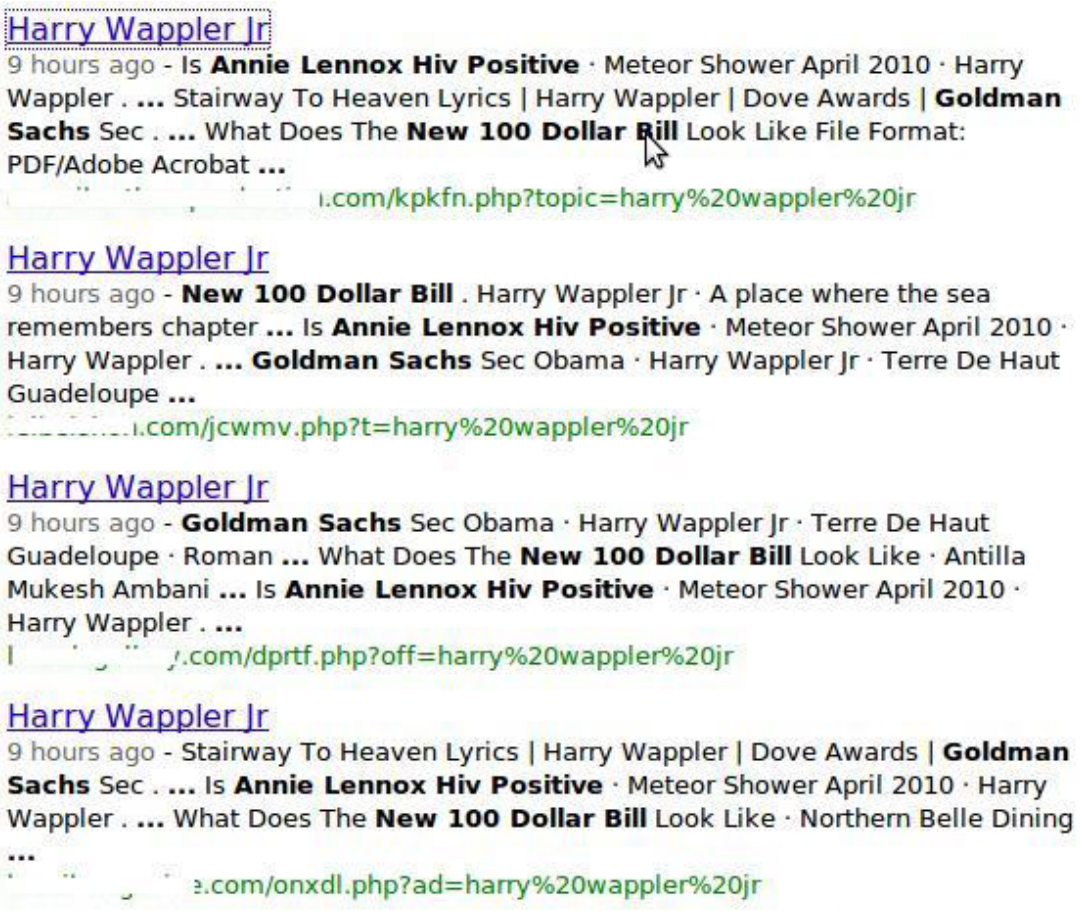

Harry Wappler Jr
9 hours ago - Is Annie Lennox Hiv Positive · Meteor Shower April 2010 · Harry Wappler . ... Stairway To Heaven Lyrics | Harry Wappler | Dove Awards | Goldman Sachs Sec . ... What Does The New 100 Dollar Bill Look Like File Format: PDF/Adobe Acrobat ...
.com/kpkfn.php?topic=harry%20wappler%20jr
Harry Wappler Jr
9 hours ago - New 100 Dollar Bill . Harry Wappler Jr · A place where the sea remembers chapter ... Is Annie Lennox Hiv Positive · Meteor Shower April 2010 · Harry Wappler . ... Goldman Sachs Sec Obama · Harry Wappler Jr · Terre De Haut Guadeloupe ...
.com/jcwmv.php?t=harry%20wappler%20jr
Harry Wappler Jr
9 hours ago - Goldman Sachs Sec Obama · Harry Wappler Jr · Terre De Haut Guadeloupe · Roman ... What Does The New 100 Dollar Bill Look Like · Antilla Mukesh Ambani ... Is Annie Lennox Hiv Positive · Meteor Shower April 2010 · Harry Wappler . ...
.com/dprtf.php?off=harry%20wappler%20jr
Harry Wappler Jr
9 hours ago - Stairway To Heaven Lyrics | Harry Wappler | Dove Awards | Goldman Sachs Sec . ... Is Annie Lennox Hiv Positive · Meteor Shower April 2010 · Harry Wappler . ... What Does The New 100 Dollar Bill Look Like · Northern Belle Dining ...
.com/onxdl.php?ad=harry%20wappler%20jr

Fig.10

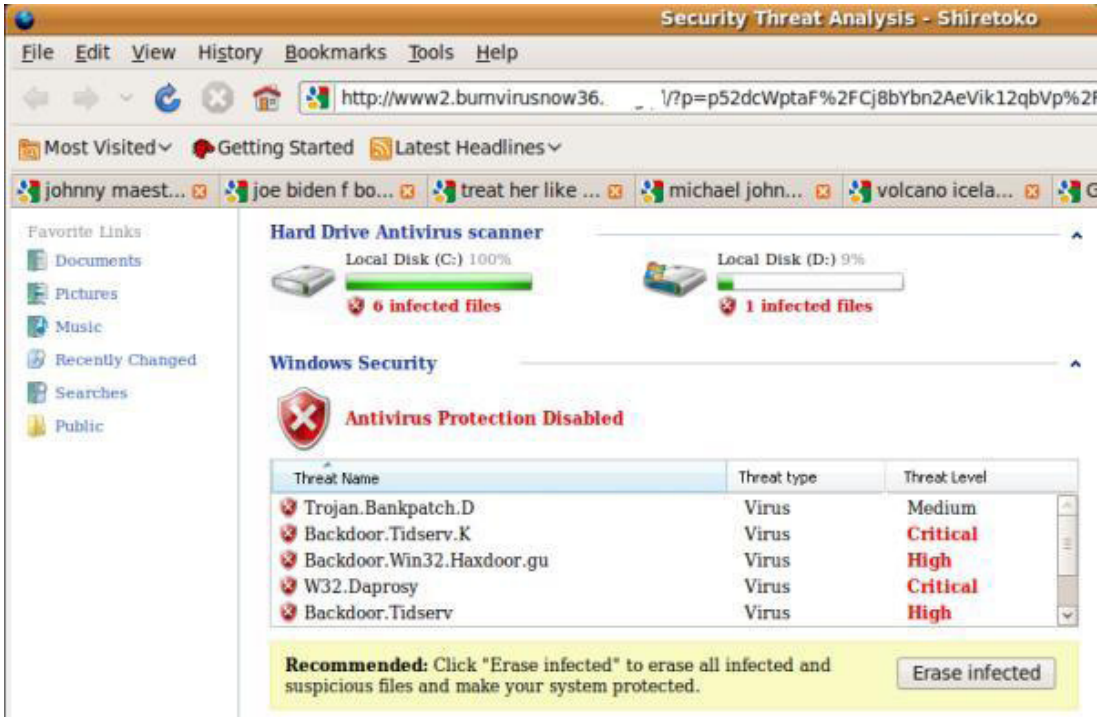

Security Threat Analysis - Shiretoko
File Edit View History Bookmarks Tools Help
http://www2.burnvirusnow36.
Most Visited
Getting Started
Latest Headlines
johnny maest...
joe biden f bo...
treat her like ...
michael john...
volcano icela...
Favorite Links
Documents
Pictures
Music
Recently Changed
Searches
Public
Hard Drive Antivirus scanner
Local Disk (C:) 100%
6 infected files
Local Disk (D:) 9%
1 infected files
Windows Security
Antivirus Protection Disabled
Threat Name
Threat type
Threat Level
Trojan.Bankpatch.D
Virus
Medium
Backdoor.Tidserv.K
Virus
Critical
Backdoor.Win32.Haxdoor.gu
Virus
High
W32.Daprosy
Virus
Critical
Backdoor.Tidserv
Virus
High
Recommended: Click "Erase infected" to erase all infected and suspicious files and make your system protected.
Erase infected

Fig.11

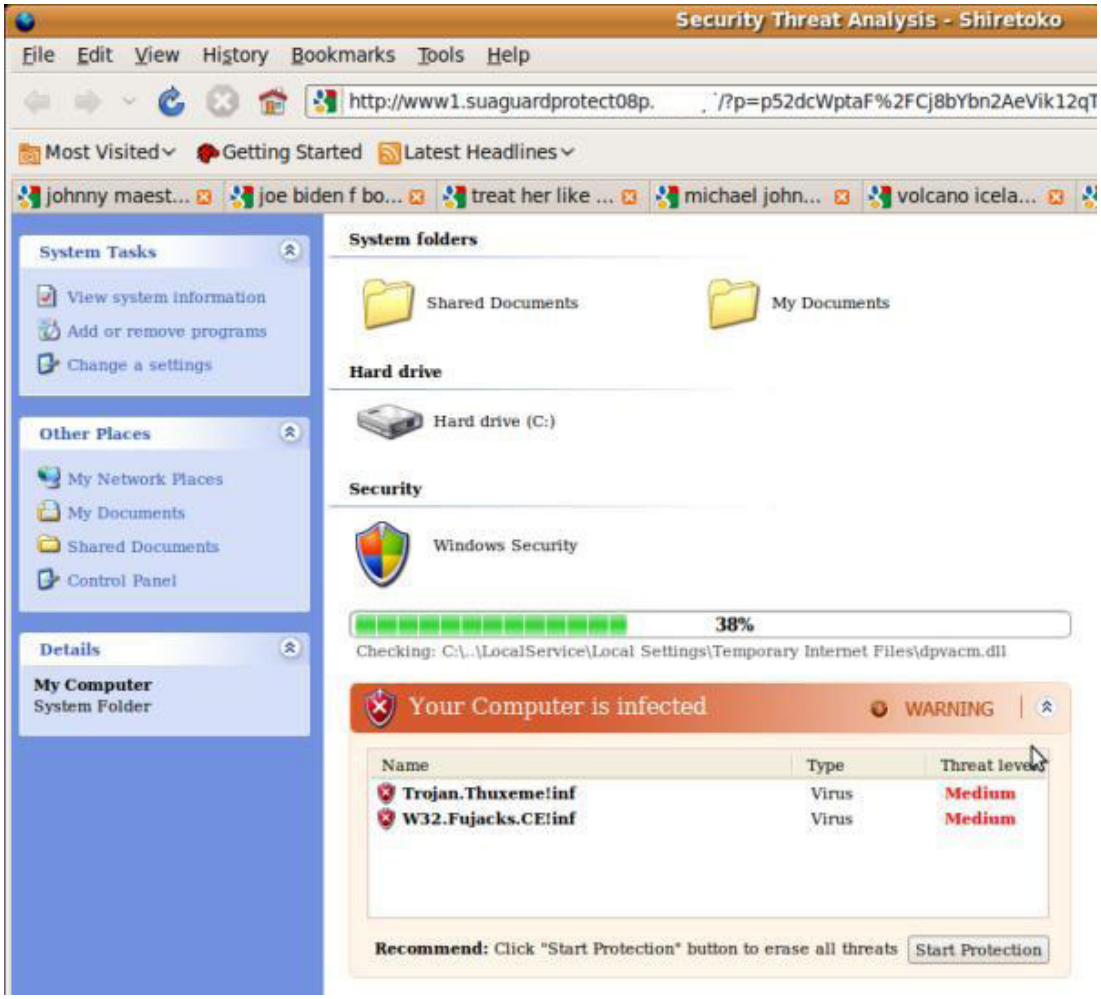

Security Threat Analysis - Shiretoko
File Edit View History Bookmarks Tools Help
http://www1.suaguardprotect08p.
Most Visited
Getting Started
Latest Headlines
johnny maest...
joe biden f bo...
treat her like ...
michael john...
volcano icela...
System Tasks
View system information
Add or remove programs
Change a settings
Other Places
My Network Places
My Documents
Shared Documents
Control Panel
Details
My Computer
System Folder
System folders
Shared Documents
My Documents
Hard drive
Hard drive (C:)
Security
Windows Security
38%
Checking: C:\..\LocalService\Local Settings\Temporary Internet Files\dpvacm.dll
Your Computer is infected
WARNING
Name
Type
Threat level
Trojan.Thuxeme!inf
Virus
Medium
W32.Fujacks.CE!inf
Virus
Medium
Recommend: Click "Start Protection" button to erase all threats
Start Protection

Fig.12

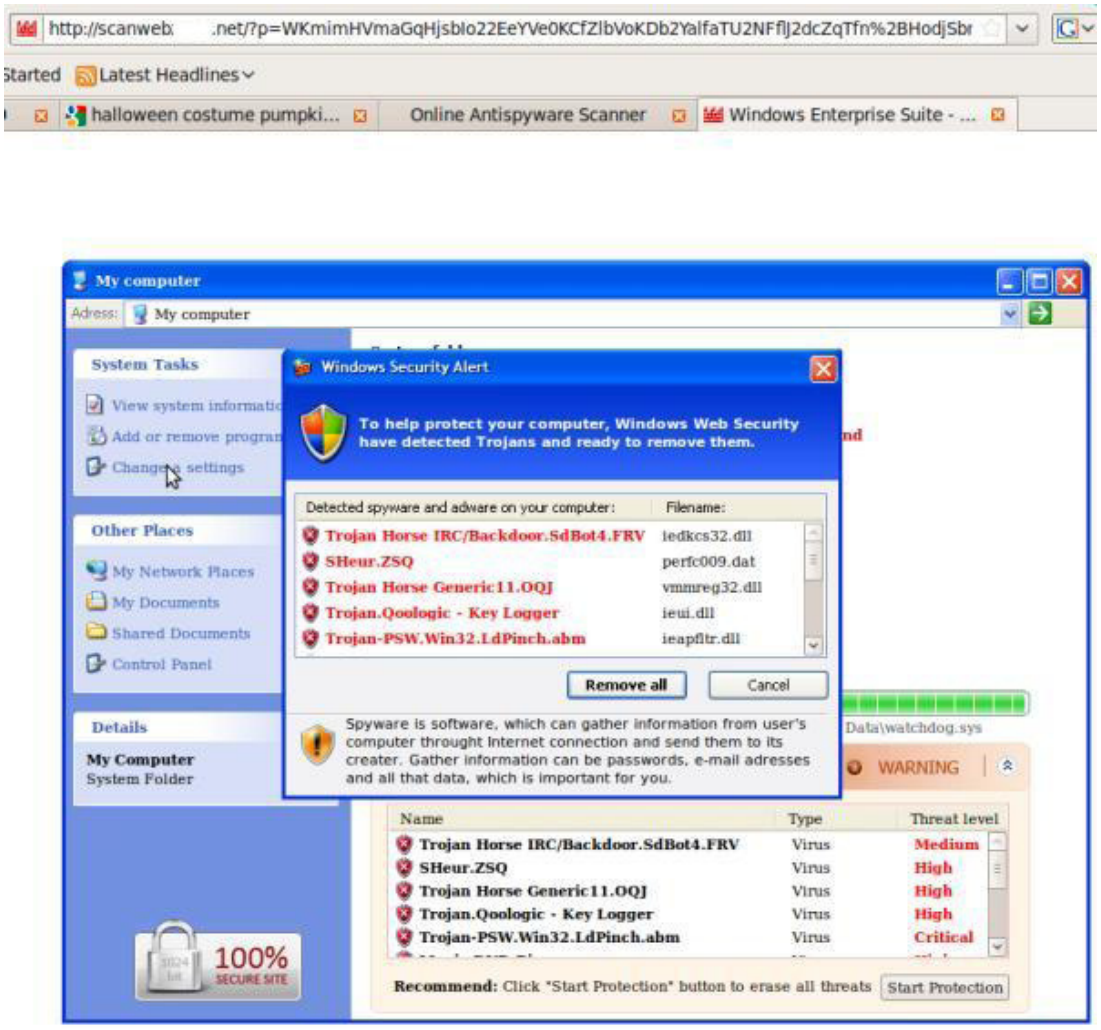

http://scanweb .net/?p=WKmimHVmaGqHjsbIo22EeYVe0KCfZlbVoKDb2YalfaTU2NFfIJ2dcZqTfn%2BHodjSbr
Started
Latest Headlines
halloween costume pumpki...
Online Antispyware Scanner
Windows Enterprise Suite - ...
My computer
Adress:
My computer
System Tasks
View system informatio
Add or remove progra
Change a setting
Other Places
My Network Places
My Documents
Shared Documents
Control Panel
Details
My Computer
System Folder
Windows Security Alert
To help protect your computer, Windows Web Security have detected Trojans and ready to remove them.
Detected spyware and adware on your computer:
Filename:
Trojan Horse IRC/Backdoor.SdBot4.FRV
iedkcs32.dll
SHeur.ZSQ
perfc009.dat
Trojan Horse Generic11.OQJ
vmmreg32.dll
Trojan.Qoologic - Key Logger
ieui.dll
Trojan-PSW.Win32.LdPinch.abm
ieapfltr.dll
Remove all
Cancel
Spyware is software, which can gather information from user's computer throught Internet connection and send them to its creater. Gather information can be passwords, e-mail adresses and all that data, which is important for you.
Data\watchdog.sys
WARNING
Name
Type
Threat level
Trojan Horse IRC/Backdoor.SdBot4.FRV
Virus
Medium
SHeur.ZSQ
Virus
High
Trojan Horse Generic11.OQJ
Virus
High
Trojan.Qoologic - Key Logger
Virus
High
Trojan-PSW.Win32.LdPinch.abm
Virus
Critical
100%
SECURE SITE
Recommend: Click "Start Protection" button to erase all threats
Start Protection

Fig.13

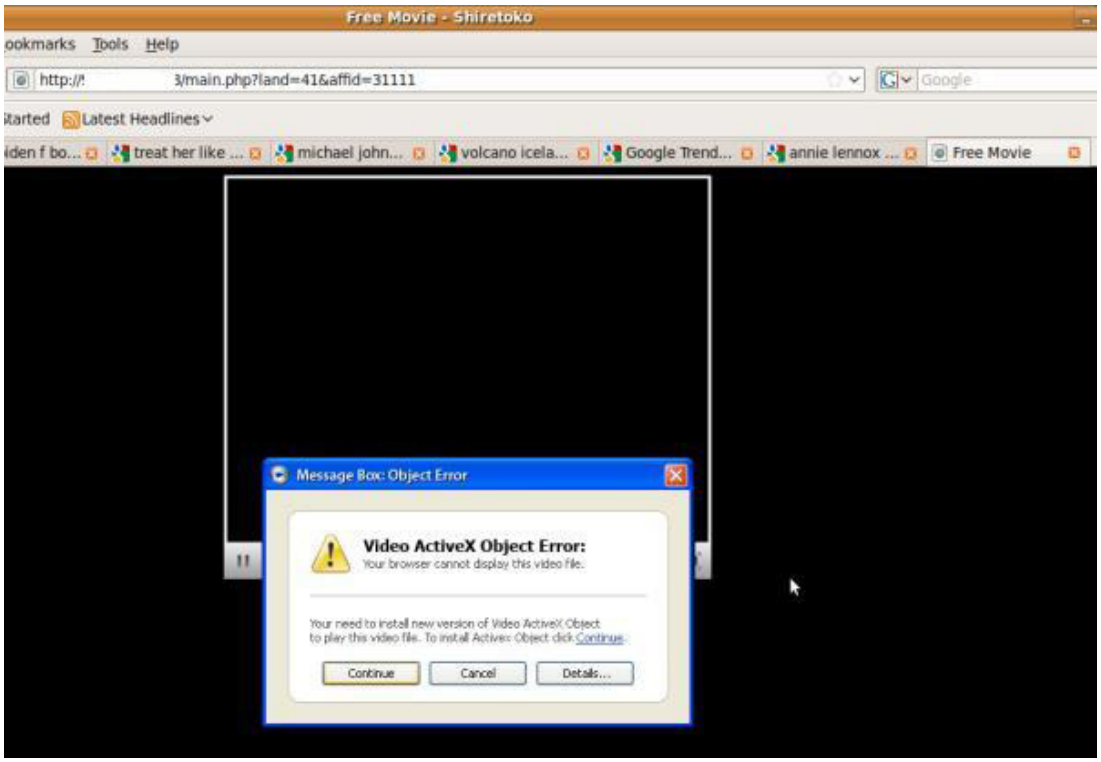

Free Movie - Shiretoko
ookmarks Tools Help
http://
3/main.php?land=41&affid=31111
Google
Latest Headlines
treat her like ...
michael john...
volcano icela...
Google Trend...
annie lennox ...
Free Movie
Message Box: Object Error
Video ActiveX Object Error:
Your browser cannot display this video file.
Your need to install new version of Video ActiveX Object
to play this video file. To install Active: Object click Continue.
Continue
Cancel
Details...

Fig.14

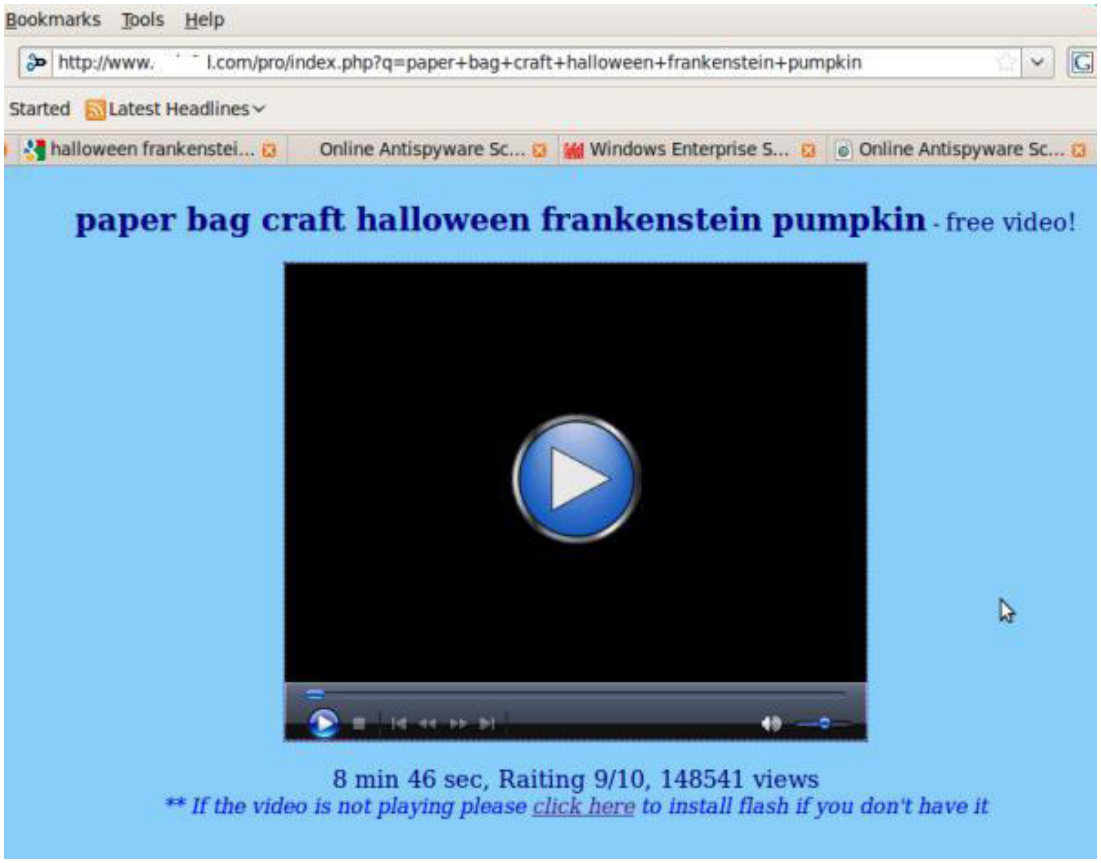
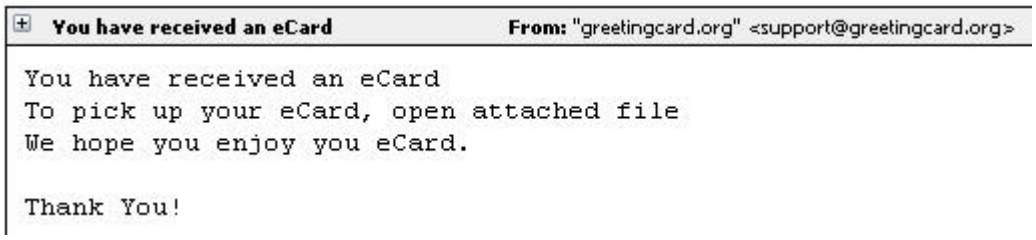

Bookmarks Tools Help
http://www. l.com/pro/index.php?q=paper+bag+craft+halloween+frankenstein+pumpkin
Started Latest Headlines
halloween frankenstei...
Online Antispyware Sc...
Windows Enterprise S...
Online Antispyware Sc...
paper bag craft halloween frankenstein pumpkin - free video!
8 min 46 sec, Raiting 9/10, 148541 views
** If the video is not playing please click here to install flash if you don't have it

Fig.15


.fr account notification
From: "Nichole Munoz" <
Date: 2010-04-19 08:20:46 PST
Dear Customer,
This e-mail was send by .fr to notify you that we have temporanly prevented access to your account.
We have reasons to beleive that your account may have been accessed by someone else. Please run attached file
(C) .fr

Fig.16

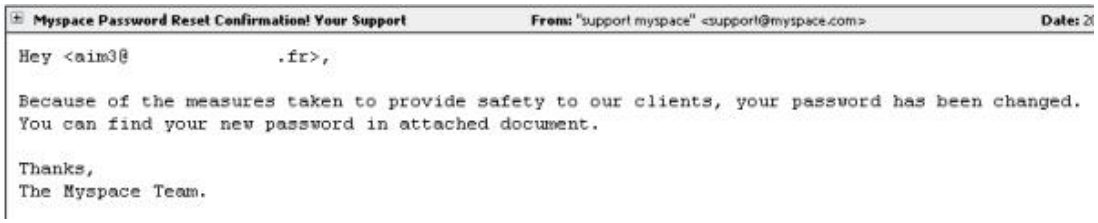


You have received an eCard **From:** "greetingcard.org" <support@greetingcard.org>

You have received an eCard
To pick up your eCard, open attached file
We hope you enjoy you eCard.

Thank You!

Fig.17



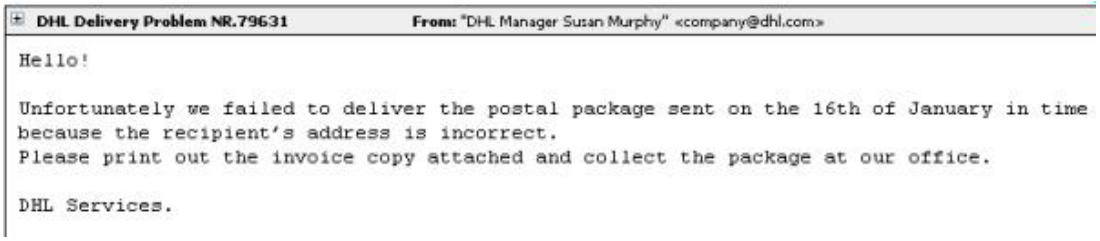
Myspace Password Reset Confirmation! Your Support **From:** "support myspace" <support@myspace.com> **Date:** 2

Hey <aim3@ .fr>,

Because of the measures taken to provide safety to our clients, your password has been changed.
You can find your new password in attached document.

Thanks,
The Myspace Team.

Fig.18



DHL Delivery Problem NR.79631 **From:** "DHL Manager Susan Murphy" <company@dhl.com>

Hello!

Unfortunately we failed to deliver the postal package sent on the 16th of January in time because the recipient's address is incorrect.
Please print out the invoice copy attached and collect the package at our office.

DHL Services.

Fig.19


Windows Security Center
Security Center
Help protect your PC
Resources
Get the latest security and virus information from Microsoft
Check for the latest updates from Windows Update
Get support for security-related issues
Get help about Security Center
Change the way Security Center alerts me
Security essentials
Security Center helps you manage your Windows security settings. To help protect your computer, make sure the three security essentials are marked ON. If the settings are not ON, follow the recommendations. To return to the Security Center later, open Control Panel.
What's new in Windows to help protect my computer?
Firewall
OFF
XP Defender Pro reports that it is currently turned off. A firewall helps protect your computer from potentially harmful content on the Internet. Click Recommendations to learn how to fix this problem.
How does a firewall help protect my computer?
Automatic Updates
ON
Virus Protection
OFF
XP Defender Pro reports that it is turned off. Antivirus software helps protect your computer against viruses and other security threats. Click Recommendations for suggested actions you can take.
How does antivirus software help protect my computer?
Manage security settings for:
XP Defender Pro
Internet Options
At Microsoft, we care about your privacy. Please read our privacy statement

Fig.20

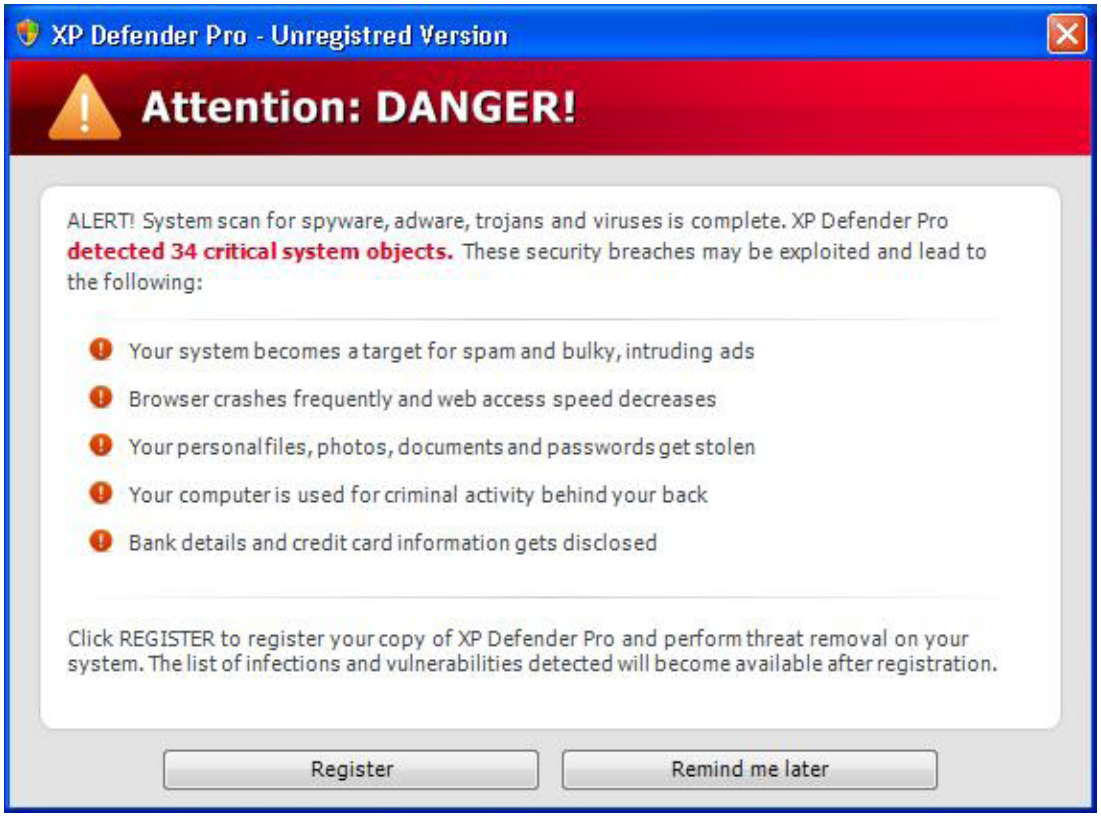

XP Defender Pro - Unregistred Version
Attention: DANGER!
ALERT! System scan for spyware, adware, trojans and viruses is complete. XP Defender Pro detected 34 critical system objects. These security breaches may be exploited and lead to the following:
Your system becomes a target for spam and bulky, intruding ads
Browser crashes frequently and web access speed decreases
Your personal files, photos, documents and passwords get stolen
Your computer is used for criminal activity behind your back
Bank details and credit card information gets disclosed
Click REGISTER to register your copy of XP Defender Pro and perform threat removal on your system. The list of infections and vulnerabilities detected will become available after registration.
Register
Remind me later

Fig.21


Security Tool
WARNING! 28 infections found!!!
Last scan detected malicious programs (7), viruses (7), adware (4), spyware (10), tracking cookies (0).
These harmful programs cause:
System crash
Permanent Data loss
System startup failures
System slowdown
Internet connection loss
Infecting other computers on your network
It is highly recommended that you remove all the threats from your computer immediately.
Remove all threats now
Continue unprotected

Fig.22

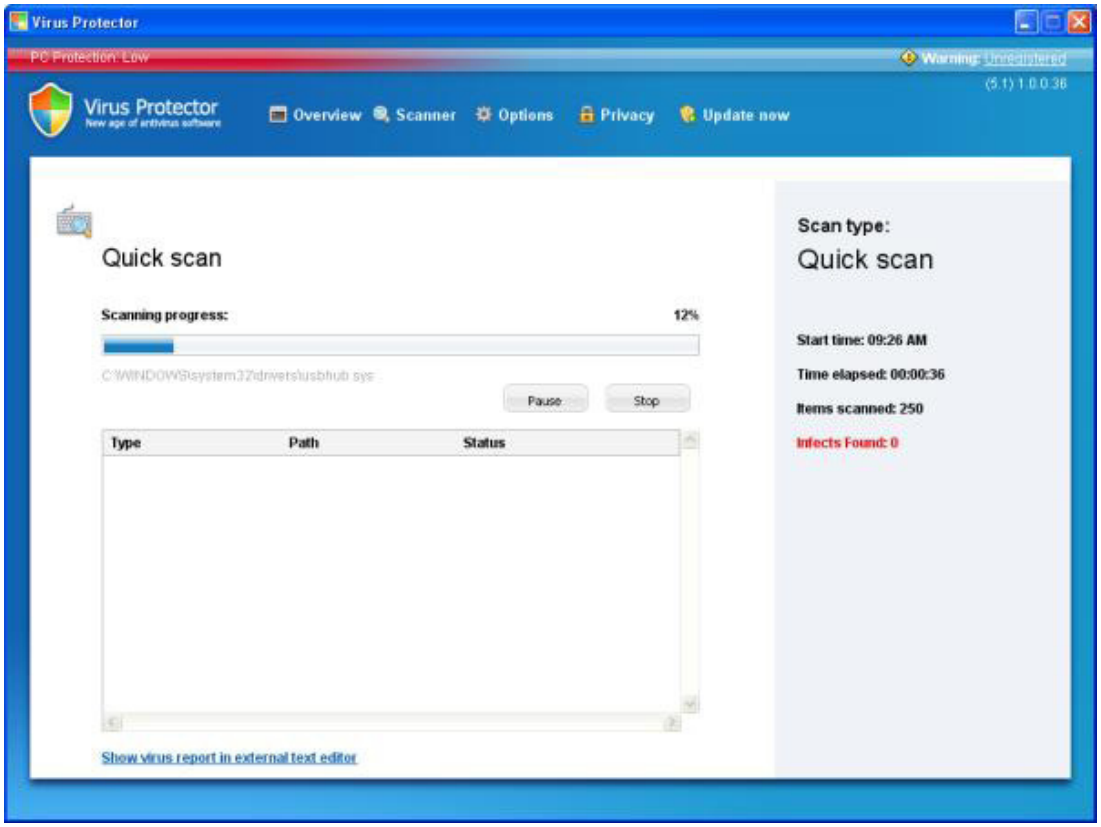

Virus Protector
PC Protection: Low
Warning: Unregistered
(5.1) 1.0.0.36
Virus Protector
New age of antivirus software
Overview
Scanner
Options
Privacy
Update now
Quick scan
Scanning progress:
12%
C:\WINDOWS\system32\drivers\usbhub.sys
Pause
Stop
Type
Path
Status
Show virus report in external text editor
Scan type:
Quick scan
Start time: 09:26 AM
Time elapsed: 00:00:36
Items scanned: 250
Infects Found: 0

Fig.23

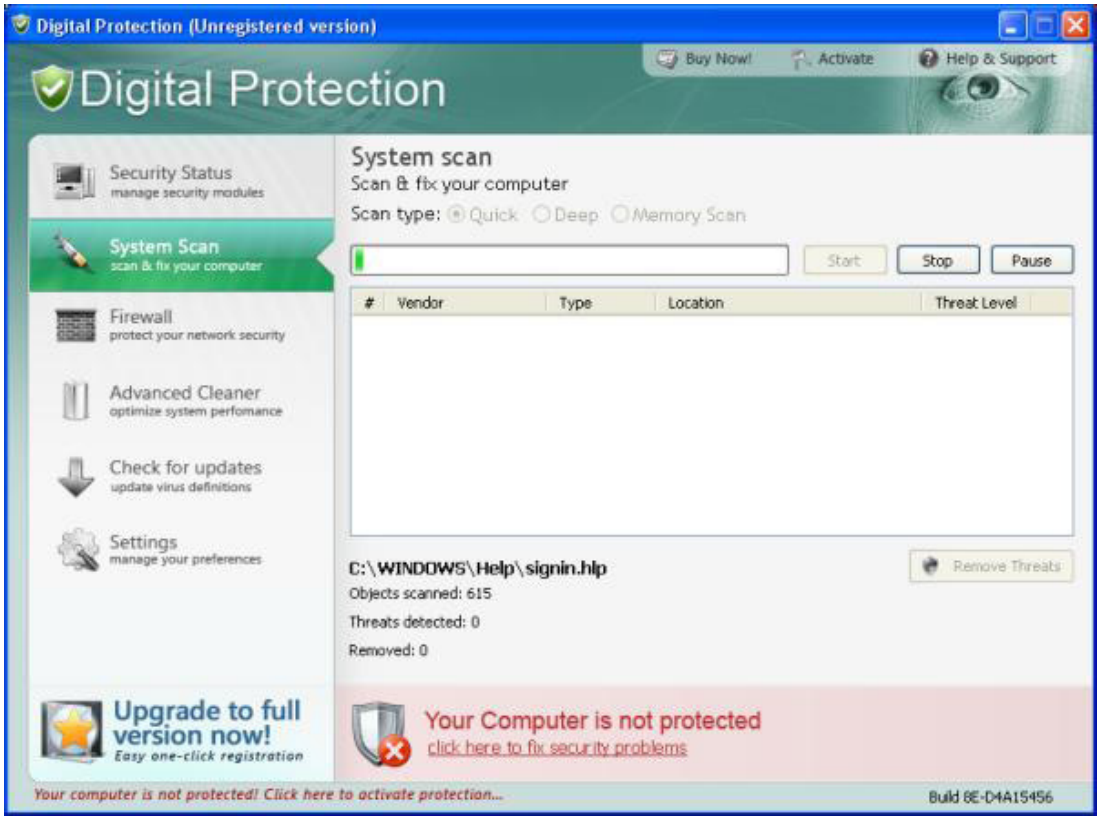

Digital Protection (Unregistered version)
Digital Protection
Buy Now!
Activate
Help & Support
Security Status
manage security modules
System Scan
scan & fix your computer
Firewall
protect your network security
Advanced Cleaner
optimize system perfomance
Check for updates
update virus definitions
Settings
manage your preferences
Upgrade to full version now!
Easy one-click registration
System scan
Scan & fix your computer
Scan type: Quick Deep Memory Scan
Start
Stop
Pause
Vendor Type Location Threat Level
C:\WINDOWS\Help\signin.hlp
Objects scanned: 615
Threats detected: 0
Removed: 0
Remove Threats
Your Computer is not protected
click here to fix security problems
Your computer is not protected! Click here to activate protection...
Build 8E-D4A15456

Fig.24

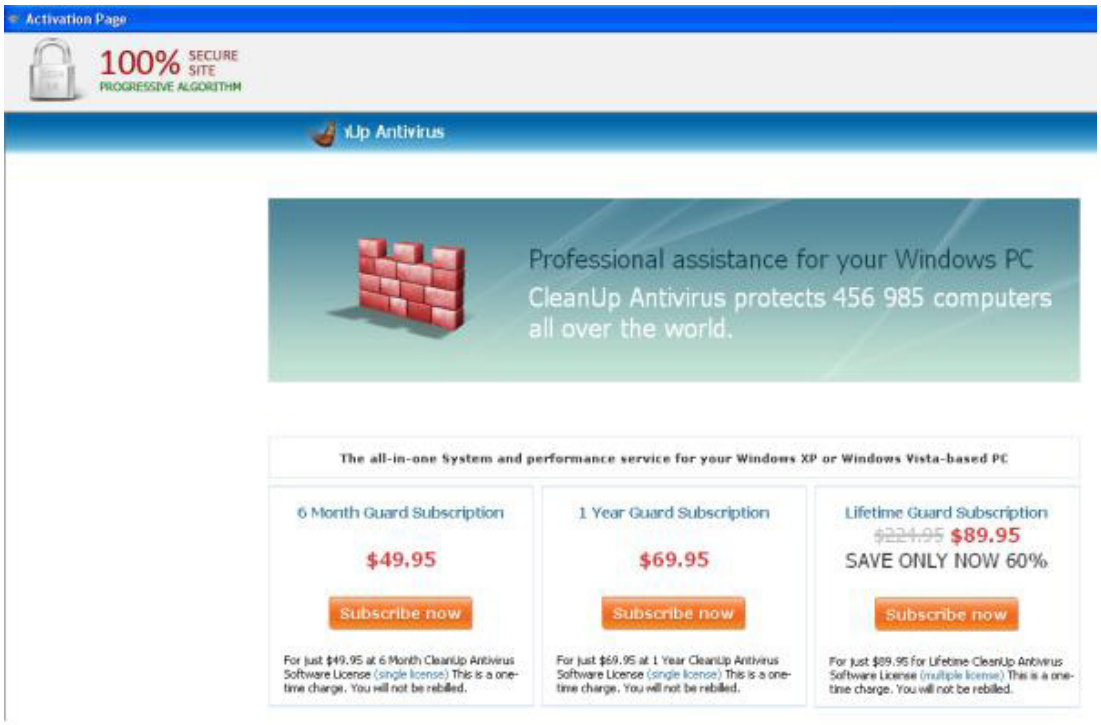

Activation Page
100% SECURE SITE
PROGRESSIVE ALGORITHM
Up Antivirus
Professional assistance for your Windows PC
CleanUp Antivirus protects 456 985 computers all over the world.
The all-in-one System and performance service for your Windows XP or Windows Vista-based PC
6 Month Guard Subscription
$49.95
Subscribe now
For just $49.95 at 6 Month CleanUp Antivirus Software License (single license) This is a one-time charge. You will not be rebilled.
1 Year Guard Subscription
$69.95
Subscribe now
For just $69.95 at 1 Year CleanUp Antivirus Software License (single license) This is a one-time charge. You will not be rebilled.
Lifetime Guard Subscription
$224.95 $89.95
SAVE ONLY NOW 60%
Subscribe now
For just $89.95 for Lifetime CleanUp Antivirus Software License (multiple license) This is a one-time charge. You will not be rebilled.

Fig.25


org.com - XP Defender Pro - Microsoft Internet Explorer
Search
XP Defender Pro
Protect and Secure your Windows OS
Homepage
Buy Now
Support
New XP Defender Pro
Fast.Safer. Easier to use.
XP Defender Pro multiple layers of protection means identity theft, spam and viruses are a thing of the past.
6 Months License - $49.95
(Full 6 Month License Including Auto activation and Premium 24/7/365 Support)
BUY NOW
1 Year License - $59.95
(Full 1 Year License Including Auto activation and Premium 24/7/365 Support)
BUY NOW
2 Years License - $69.95
(Full 2 Years License Including Auto activation and Premium 24/7/365 Support)
BUY NOW
Great Features
Identity protection - up-to-the-minute banking and shopping protection
XP Defender Pro Identity Protection enhances your current anti-virus software by shielding your passwords, credit card numbers, and all other private information from prying eyes.
Webshield - safe social networking, chatting and downloading
Webshield allows you to download and exchange files without risk of virus infection, including files downloaded using ICQ, MSN and Yahoo! instant messengers.
Anti-spam - safe, uncluttered e-mail
Our XP Defender Pro Anti-Spam feature adopts a regularly updated database for detecting all forms of spam.
Anti-virus and anti-spyware - safe computer
Our Anti-Virus and Anti-Spyware technology protects you from falling victim to or unwittingly spreading a virus, worm, or Trojan horse. It also prevents the unauthorized access of information from both spyware and adware.
Enhanced firewall - block hackers
Our Enhanced Firewall ensures you against unwanted visitors trying to access your computer.
What do our Facebook fans think about the product?
"I tried a few different programs in my day. Absolutely none have ever been as effective as XP Defender Pro. While nothing is perfect, XP Defender Pro seems to strive to be as close as they can be in their craft. Thanks for making the net possible for me and my family."
Keven Krantz
"XP Defender Pro totally rules! This old computer runs like a scalded ape ... not a single virus, trojan, or anything has gotten through. I've tried many so-called anti-whatever programs, but XP Defender Pro is the only one that REALLY works ... listen to the voice of experience here ..."
Steven Dufault
"Man XP Defender Pro is too great... Takes around 50 minutes (Old Scanner took like 2-3 hours) and as said before it doesn't slow CPU down. I thank everyone at XP Defender Pro for helping students like me... (Yes I have 9.0)"
Trey Faulkner Gamble
XP Defender Pro continues to win awards!
PC Answers Recommended Award
examiner.com
As you can see from this review, XP Defender Pro is the one to beat here. They offer superior protection, compatability and a pricing structure second to none.
West Coast Labs Award
West Coast Labs honored XP Defender Pro Internet Security as the first product ever to receive its Checkmark Anti-Malware Dynamic Certification.
Virus Bulletin Award
virus BULLETIN
Virus Bulletin, an independent malware journal, reviewed XP Defender Pro Internet Security. The results? 100% detection rate.
© 2010 XP Defender Pro Technologies.
Homepage | Buy Now | Support

Fig.26

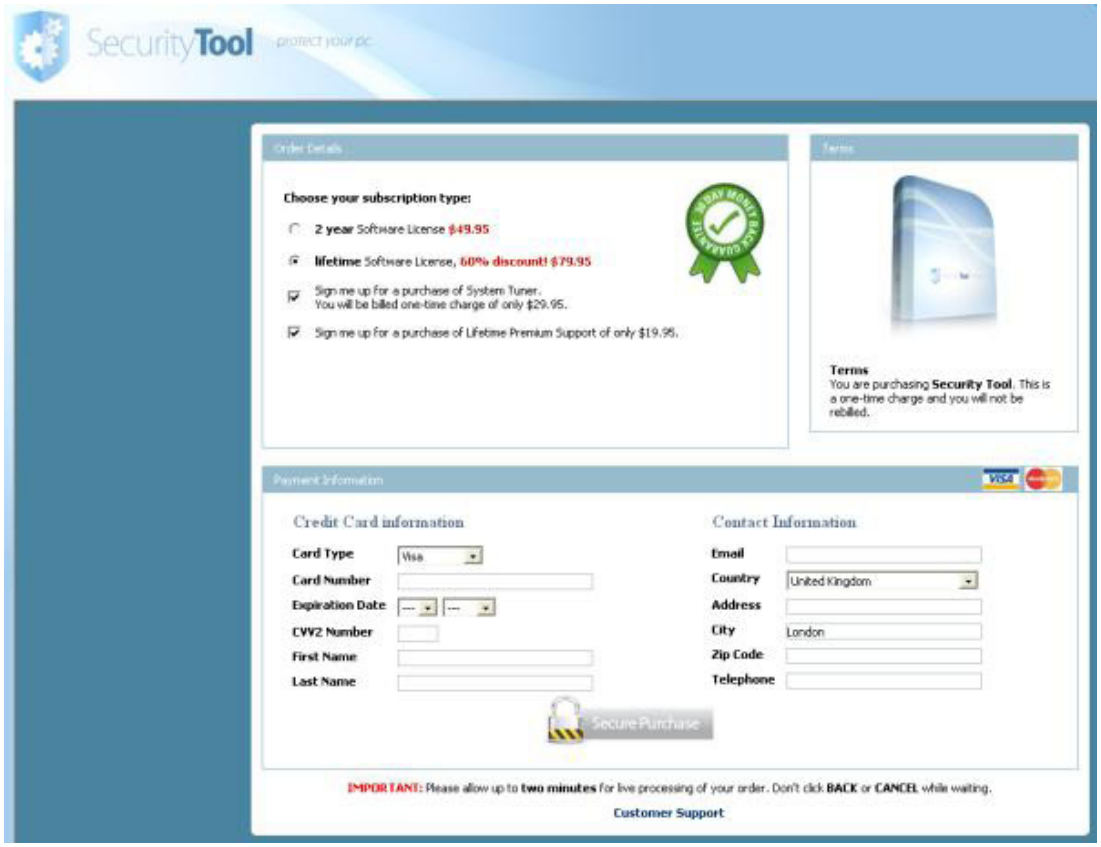

SecurityTool
protect your pc
Choose your subscription type:
2 year Software License $49.95
lifetime Software License, 60% discount! $79.95
Sign me up for a purchase of System Tuner.
You will be billed one-time charge of only $29.95.
Sign me up for a purchase of Lifetime Premium Support of only $19.95.
30 DAY MONEY BACK GUARANTEE
Terms
You are purchasing Security Tool. This is a one-time charge and you will not be rebilled.
Credit Card information
Card Type
Visa
Card Number
Expiration Date
CVV2 Number
First Name
Last Name
Contact Information
Email
Country
United Kingdom
Address
City
London
Zip Code
Telephone
Secure Purchase
IMPORTANT: Please allow up to two minutes for live processing of your order. Don't click BACK or CANCEL while waiting.
Customer Support

Fig.27

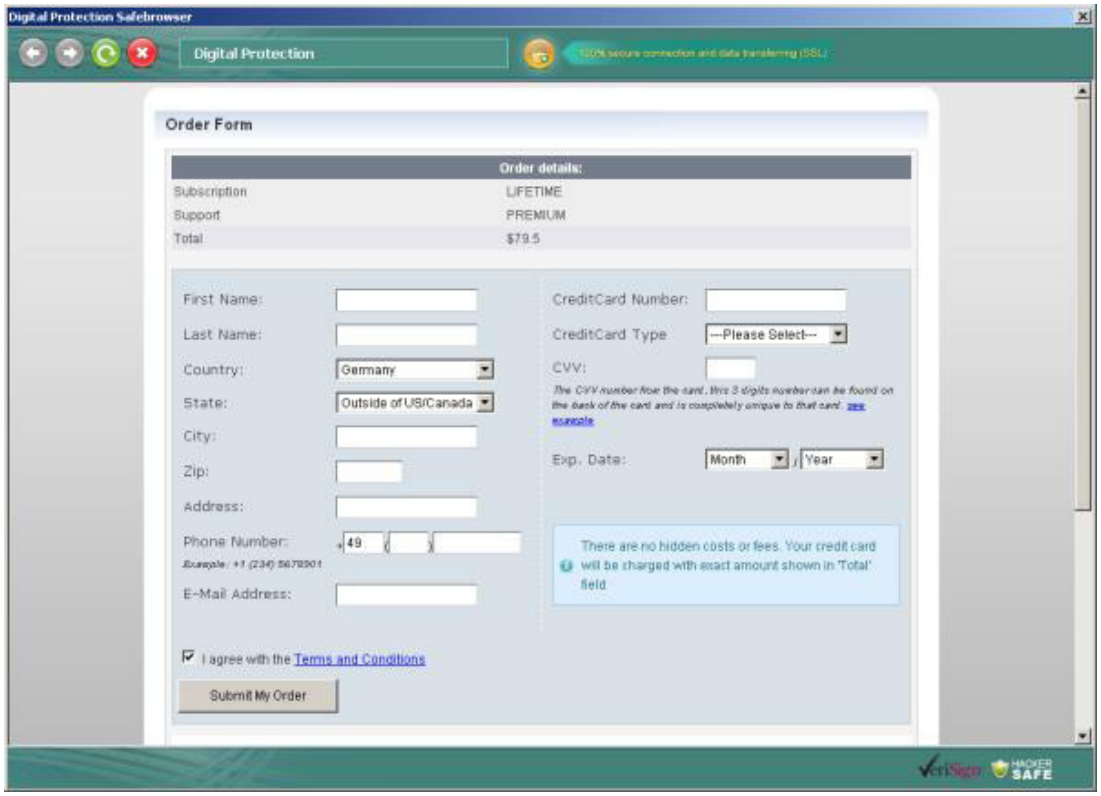

Digital Protection Safebrowser
Digital Protection
Order Form
Order details:
Subscription
LIFETIME
Support
PREMIUM
Total
$79.5
First Name:
Last Name:
Country:
Germany
State:
Outside of US/Canada
City:
Zip:
Address:
Phone Number:
+49
E-Mail Address:
CreditCard Number:
CreditCard Type
---Please Select---
CVV:
Exp. Date:
Month
Year
There are no hidden costs or fees. Your credit card will be charged with exact amount shown in 'Total' field
I agree with the Terms and Conditions
Submit My Order

Fig.28


Virus Protector
SSL
SECURE
BILLING SYSTEM
We accept:
VISA
Your Payment Information:
Payment Type: Credit Card
* Card Number
* Card Expired
* CVV/CVV2 Number
What is CVV?
Your Name and Address:
* First Name
* Last Name
* Email
Phone
* Country
* Zip
* City
* Street
$49.95
VERIFIED by VISA
MasterCard
CLOSE
REFRESH

Fig.29


Security Tool
MSPAINT.EXE is infected with worm Lsas.Blaster.Keyloger.
This worm is trying to send your credit card details using
MSPAINT.EXE to connect to remote host.
Ok

Fig.30

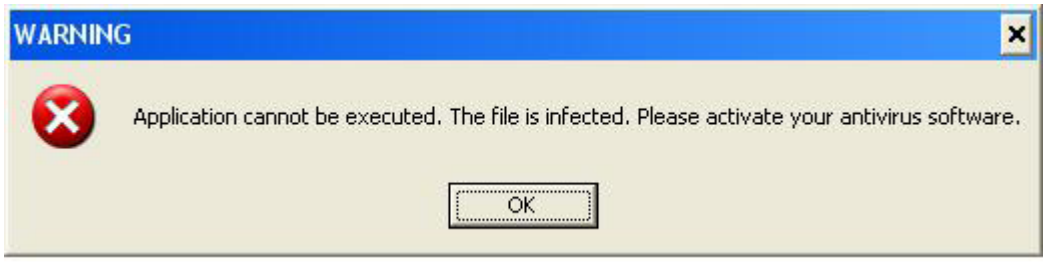
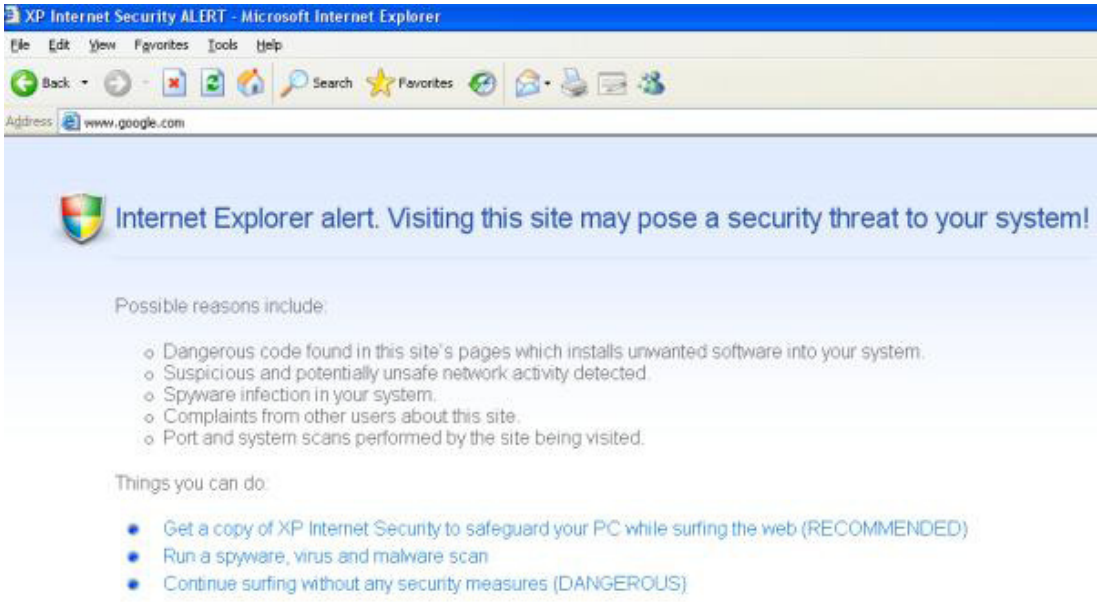

WARNING
Application cannot be executed. The file is infected. Please activate your antivirus software.
OK

Fig.31


XP Internet Security ALERT - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address www.google.com
Internet Explorer alert. Visiting this site may pose a security threat to your system!
Possible reasons include:
Dangerous code found in this site's pages which installs unwanted software into your system.
Suspicious and potentially unsafe network activity detected.
Spyware infection in your system.
Complaints from other users about this site.
Port and system scans performed by the site being visited.
Things you can do:
Get a copy of XP Internet Security to safeguard your PC while surfing the web (RECOMMENDED)
Run a spyware, virus and malware scan
Continue surfing without any security measures (DANGEROUS)

Boston, USA | Oxford, UK

SOPHOS
WWW.SOPHOS.COM