SOPHOS

simple + secure

Stopping Fake Antivirus: How to Keep Scareware off Your Network

Fake antivirus is one of the most frequently encountered threats on the web today. Also known as rogue antivirus, rogues, or scareware, fake antivirus uses social engineering to lure users to malicious sites and scare them into paying for fake threat removal tools.

This paper provides insight into where fake antivirus comes from and how it is distributed, what happens when a system is infected with fake antivirus, and how to stop this persistent threat from infecting your network and your users.

What is fake antivirus?

Fake antivirus is fake security software which pretends to find dangerous security threats—such as viruses—on your computer. The initial scan is free, but if you want to clean up the fraudulently-reported "threats," you need to pay.

This class of malware displays false alert messages to computer users concerning threats on their machines (but these threats do not really exist). The 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 fake antivirus malware will continue to send these annoying and intrusive alerts until a payment is made or the malware is removed.

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

Why is fake antivirus so popular among cybercriminals? It is a huge revenue source. Compared to other classes of malware such as bots, backdoor Trojans, downloaders and password stealers, fake antivirus draws the victim into handing money over directly to the malware author. Victims typically pay around $120 via credit card to pay for the junk software that will supposedly fix the problem.

Fake antivirus 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]. Individual affiliates can quickly generate income because distribution networks pay affiliates between $25 and $35 to simply do "lead generation" by infecting additional computers.

At SophosLabs, we are seeing new and different types of fake antivirus emerging. Macs are now a major target, including Mac-targeted social engineering being used from the bait to the malware. We have been carefully tracking the developments in the Mac OS X malware community, and have concluded that fake antivirus for Macs is advancing fast and taking many cues from the Windows malware scene.

Hackers are also using image and image search poisoning in addition to trending topics to infect users with fake antivirus. In addition, SophosLabs is seeing prolific rebranding of fake antivirus names to confuse users and elude detection.

Typical signs of infection

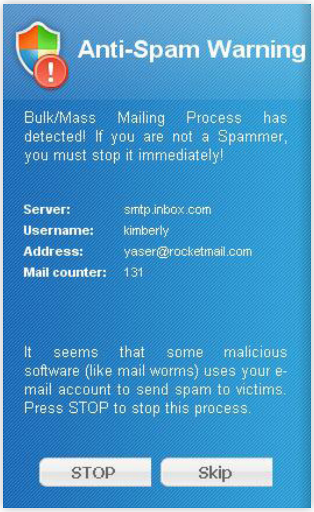
Fake antivirus usually uses a large array of social engineering techniques to get itself installed. Campaigns have included:

- 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 fake antivirus families will display popup messages (see fig.1-5).



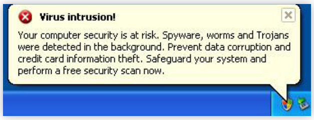
Anti-Spam Warning

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.

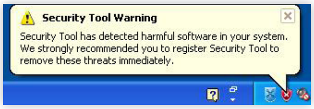
Fig.1



Virus intrusion!

Your computer security is at risk. Spyware, worms and Trojans were detected in the background. Prevent data corruption and credit card information theft. Safeguard your system and perform a free security scan now.

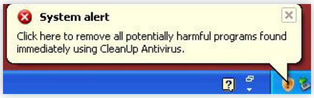
Fig.2



Security Tool Warning

Security Tool has detected harmful software in your system. We strongly recommended you to register Security Tool to remove these threats immediately.

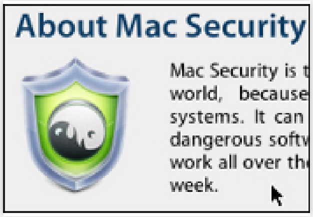
Fig.3



System alert

Click here to remove all potentially harmful programs found immediately using CleanUp Antivirus.

Fig.4



About Mac Security

Mac Security is t
world, because
systems. It can
dangerous softw
work all over th
week.

Fig.5

Fake scanning

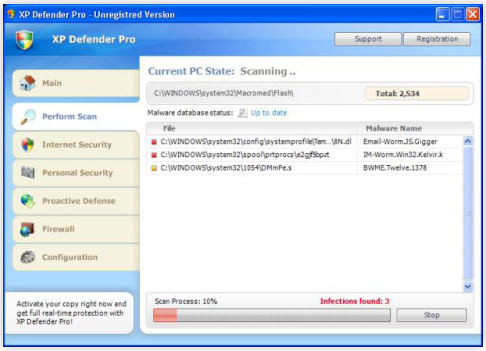
The fake antivirus will typically pretend to scan the computer and find non-existent threats, sometimes creating files full of junk that will then be detected[6] (see fig.6-8).

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

- Security Shield
- Windows XP Recovery
- Security Tool
- Internet Defender
- PC Security Guardian
- BitDefender 2011
- Security Defender
- Antimalware Tool
- Smart Internet Protection
- AntiVirus AntiSpyware 2011
- Malware Protection
- XP Security 2012
- Security Protection
- XP Antivirus 2012
- XP Anti-Spyware 2011
- MacDefender
- Mac Security

There can be many thousands of variants for each family as techniques such as server-side polymorphism are used heavily to alter the fake antivirus 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.



Current PC State: Scanning ..

C:\WINDOWS\system32\Macromed\Flash\ Total: 2,534

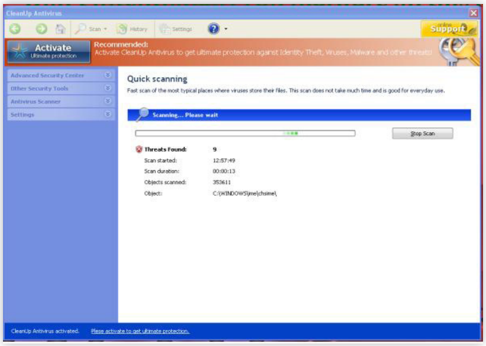
Malware database status: Up to date

File	Malware Name
C:\WINDOWS\system32\config\systemprofile\Tem...\8N.dl	Email-Worm.JS.Gigger
C:\WINDOWS\system32\spool\prtprocs\e2gjf5bp.t	IM-Worm.Win32.Kelvir.k
C:\WINDOWS\system32\1054\DMmPe.s	BWME.Twelve.1378

Scan Process: 10% Infections found: 3

Activate your copy right now and get full real-time protection with XP Defender Pro!

Fig.6



Recommended:
Activate CleanUp Antivirus to get ultimate protection against Identity Theft, Viruses, Malware and other threats!

Quick scanning

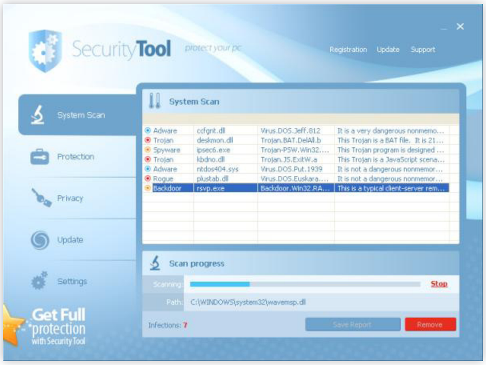
Fast scan of the most typical places where viruses store their files. This scan does not take much time and is good for everyday use.

Scanning... Please wait

Threats Found:	9
Scan started:	12:57:49
Scan duration:	00:00:13
Objects scanned:	353611
Object:	C:\WINDOWS\ime\chsime\

CleanUp Antivirus activated. Plese activate to get ultimate protection.

Fig.7



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...

Scanning:

Path: C:\WINDOWS\system32\wavemsp.dll

Infections: 7

Fig.8

Infection vectors

How do people get infected with fake antivirus?

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

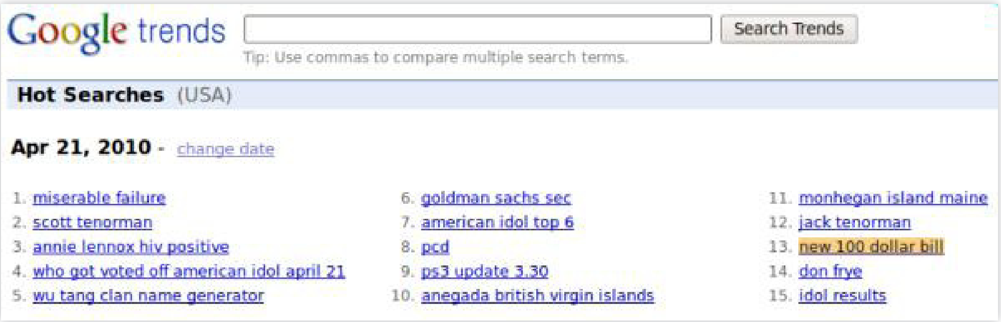
In this paper, we review several main sources of fake antivirus infection:

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

Search engine optimization poisoning

A very common source of fake antivirus infection is clicking on links received from popular search engines while searching for topical terms. Fake antivirus authors ensure that links leading to fake antivirus download sites will feature prominently in search results by using Black Hat SEO techniques[8]. These poisoned results will redirect users to a fake antivirus-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 fake antivirus installer.

Google Trends 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 fake antivirus authors. Let's do a search for pages containing terms from Hot Searches (see fig.9).



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

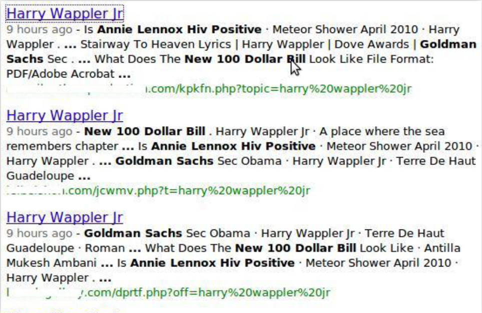
Fig.9

Picking several of the terms and performing a search for them will produce several poisoned results (see fig.10).

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 (see fig.11-13).

Or, users are taken to a fake movie download page where they are told they need to download a codec to view the movie (see fig.14, 15).

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

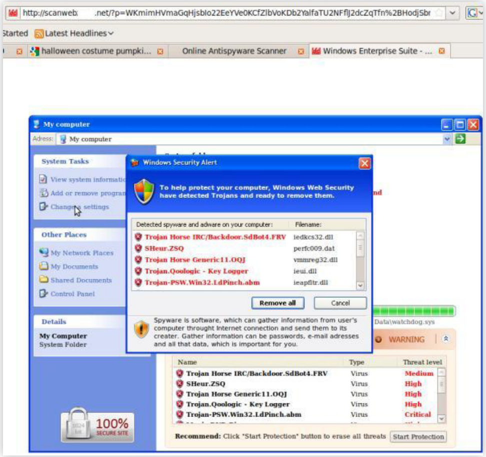


Harry Wappler Jr
9 hours ago - Is **Annie Lennox Hiv Positive** · Meteor Shower April 2010 · Harry Wappler . **...** Stairway To Heaven Lyrics | Harry Wappler | Dove Awards | **Goldman Sachs** Sec . **...** What Does The **New 100 Dollar Bill** Look Like File Format: PDF/Adobe Acrobat **...**
.com/kpkfn.php?topic=harry%20wappler%20jr

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

Fig.10



http://scanweb .net/?p=WKmimHVmaGqHjsblo22EeYVe0KCfZlbVoKDb2YalfaTU2NFflJ2dcZqTfn%2BHodjSbr

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

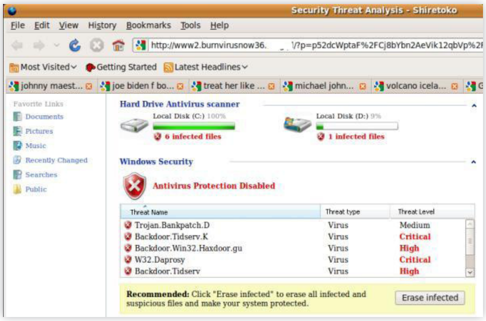
Spyware is software, which can gather information from user's computer throught Internet connection and send them to its creater. Gather information can be passwords, e-mail adresses and all that data, which is important for you.

Data\watchdog.sys

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

Recommend: Click "Start Protection" button to erase all threats

Fig.11



Security Threat Analysis - Shiretoko

http://www2.burnvirusnow36. \/?p=p52dcWptaF%2FCj8bYbn2AeVik12qbVp%2F

Hard Drive Antivirus scanner

Local Disk (C:) 100%
6 infected files

Local Disk (D:) 9%
1 infected files

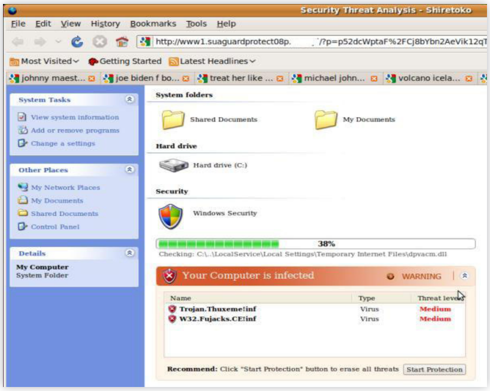
Windows Security

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.

Fig.12



Security Threat Analysis - Shiretoko

http://www1.suaguardprotect08p. /?p=p52dcWptaF%2FCj8bYbn2AeVik12qT

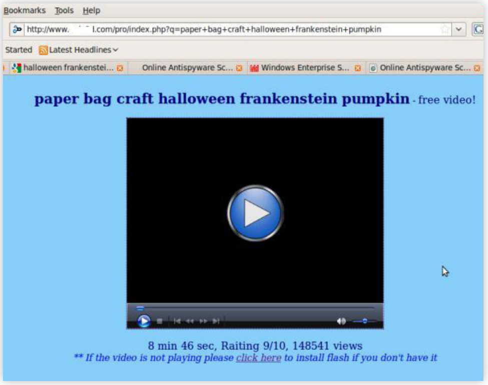
38%
Checking: C:\..\LocalService\Local Settings\Temporary Internet Files\dpvacm.dll

Your Computer is infected

Name	Type	Threat level
Trojan.Thuxeme!inf	Virus	Medium
W32.Fujacks.CE!inf	Virus	Medium

Recommend: Click "Start Protection" button to erase all threats

Fig.13

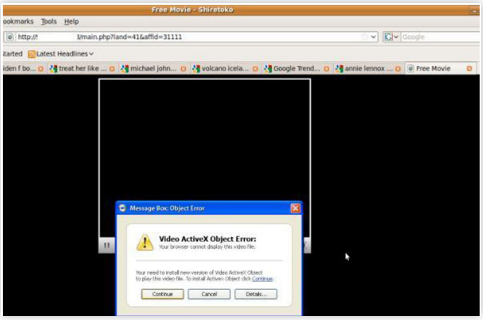


http://www. l.com/pro/index.php?q=paper+bag+craft+halloween+frankenstein+pumpkin

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.14



Free Movie - Shiretoko

http:// 3/main.php?land=41&affid=31111

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 Activex Object click Continue.

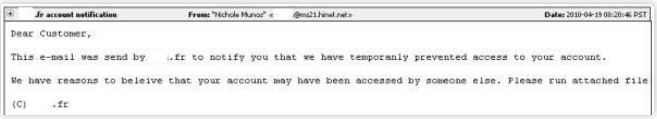
Fig.15

Spam campaigns

Fake antivirus 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 fake antivirus, 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 fake antivirus 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 (see fig.16).
- Ecard scams: An email is received purporting to be from a legitimate ecard company. In fact, a fake antivirus installer is attached (see fig.17).
- 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 (see fig.18).
- Package delivery scam: Details of a (fictitious) recent postal delivery are included in an attached file. In reality, the attachment will install fake antivirus (see fig.19).



.fr account notification **From:** "Nichole Munoz" < @ms21.hinet.net> **Date:** 2010-04-19 08:20:46 PST

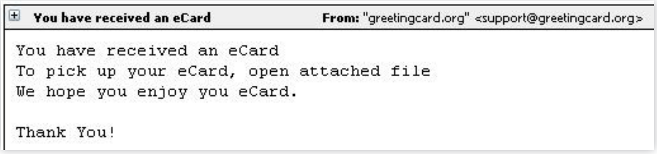
```
Dear Customer,

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

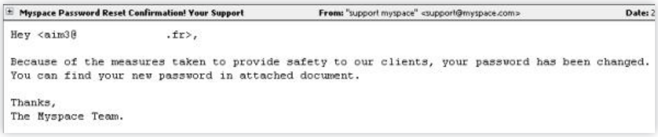


You have received an eCard **From:** "greetingcard.org" <support@greetingcard.org>

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

Thank You!
```

Fig.17



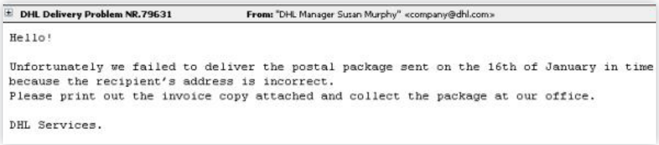
Myspace Password Reset Confirmation! Your Support **From:** "support myspace" <support@myspace.com> **Date:** 2

```
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

Compromised websites and exploit payloads

Users can sometimes be sent to fake antivirus 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 fake antivirus. 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 fake antivirus binary as the payload or a simple iframe that redirects the browser to a fake antivirus web page[12, 13].

Fake antivirus downloads by other malware

Fake antivirus 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 fake antivirus onto an infected machine, most notably TDSS, Virtumundo and Waled[14]. The infamous Conficker worm was also observed to install fake antivirus 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 fake antivirus.

In addition a pay-per-install model exists where hackers are paid to infect users' computers. In this system, a hacker controls a victim's computer (using TDSS or similar), and is paid by the fake antivirus producer to install the fake antivirus on the infected computer.

Fake antivirus families

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

Registry installation

Fake antivirus'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 fake antivirus 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\Runwpkarufv

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

HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnceCUA

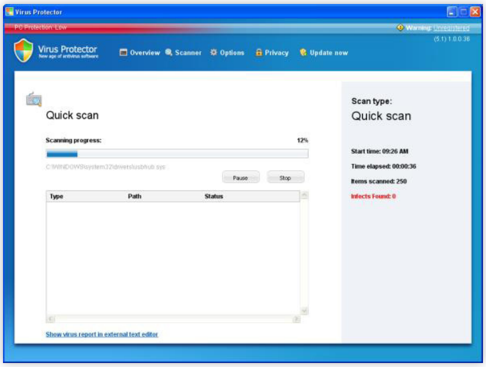
c:\windows\temp\sample.exe

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run85357230

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

Initiate a fake scan

Once fake antivirus 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 fake antivirus window is often very professionally created and victims can easily be convinced that they are using a genuine security product (see fig.20-25).


Virus Protector

PC Protection: Low

Warning: Unregistered

(5.1) 1.0.0.36

Virus Protector
New age of antivirus software

Quick scan

Scanning progress: 12%

C:\WINDOWS\system32\drivers\usbhub.sys

Type	Path	Status

Show virus report in external text editor

Scan type:
Quick scan

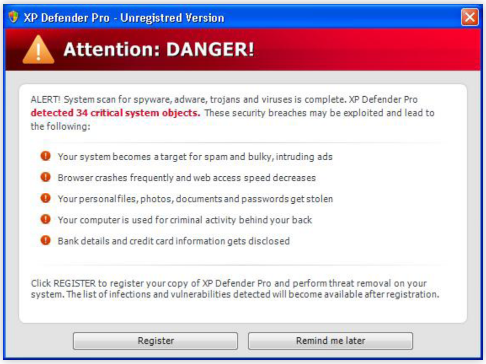
Start time: 09:26 AM

Time elapsed: 00:00:36

Items scanned: 250

Infects Found: 0

Fig.20


XP Defender Pro - Unregistred Version

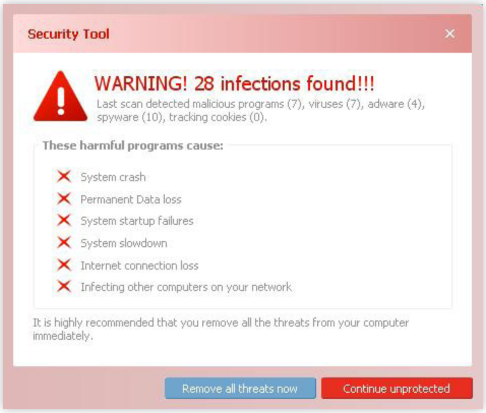
Attention: DANGER!

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.

Fig.21


Security Tool

WARNING! 28 infections found!!!

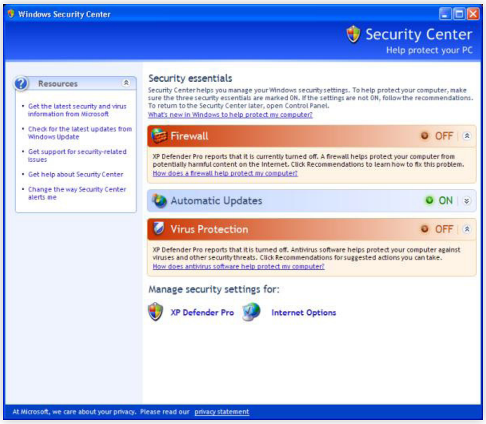
Last scan detected malicious programs (7), viruses (7), adware (4), spyware (10), tracking cookies (0).

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.

Fig.22


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

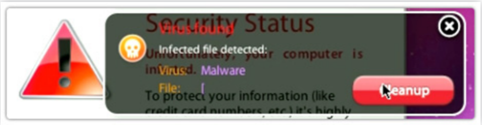
XP Defender Pro reports that it is turned off. Antivirus software helps protect your computer against viruses and other security threats. Click Recommendations for suggested actions you can take.
How does antivirus software help protect my computer?

Manage security settings for:

XP Defender Pro   Internet Options

At Microsoft, we care about your privacy. Please read our privacy statement

Fig.23


Security Status

Virus found

Infected file detected:

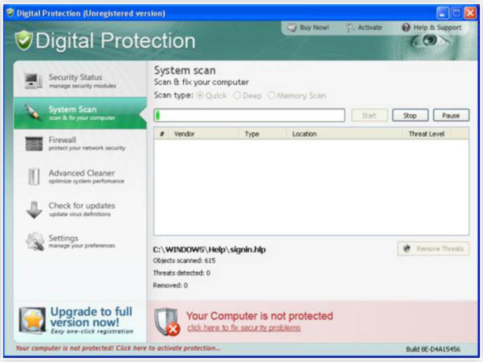
Unfortunately, your computer is infected.

Virus: Malware

File: [

To protect your information (like credit card numbers, etc.) it's highly

Fig.24


Digital Protection (Unregistered version)

Digital Protection

System scan
Scan & fix your computer

Scan type: ● Quick ○ Deep ○ Memory Scan

#	Vendor	Type	Location	Threat Level

C:\WINDOWS\Help\signin.hlp

Objects scanned: 615

Threats detected: 0

Removed: 0

Upgrade to full version now!
Easy one-click registration

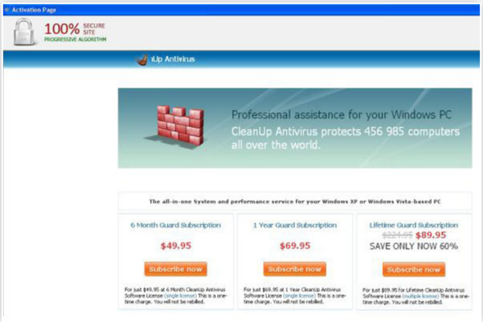
Your Computer is not protected
click here to fix security problems

Your computer is not protected! Click here to activate protection...

Build 8E-D4A15456

Fig.25

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 fake antivirus 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] (see fig.26-31).

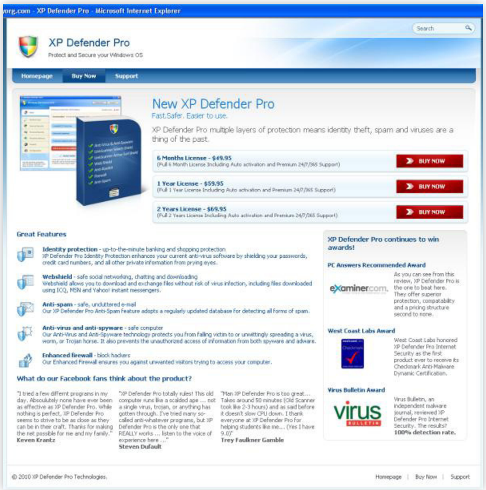


Professional assistance for your Windows PC
CleanUp Antivirus protects 456 985 computers all over the world.

The all-in-one System and performance service for your Windows XP or Windows Vista-based PC

6 Month Guard Subscription	1 Year Guard Subscription	Lifetime Guard Subscription
$49.95	$69.95	~~$224.95~~ $89.95 SAVE ONLY NOW 60%
Subscribe now	Subscribe now	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.	For just $69.95 at 1 Year CleanUp Antivirus Software License (single license) This is a one-time charge. You will not be rebilled.	For just $89.95 for Lifetime CleanUp Antivirus Software License (multiple license) This is a one-time charge. You will not be rebilled.

Fig.26



XP Defender Pro
Protect and Secure your Windows OS

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 differnt programs in my day. Absoulutely 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!

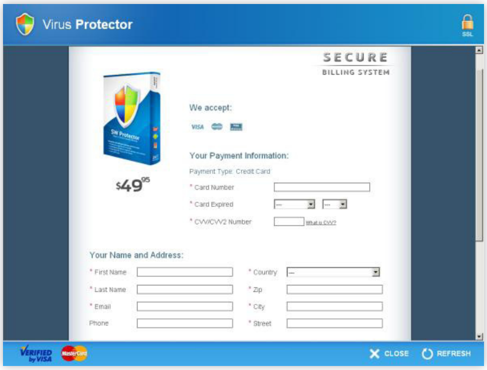
PC Answers Recommended Award
As you can see from this review, XP Defender Pro is the one to beat here. They offer superior protection, compatablity and a pricing structure second to none.

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, 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.27

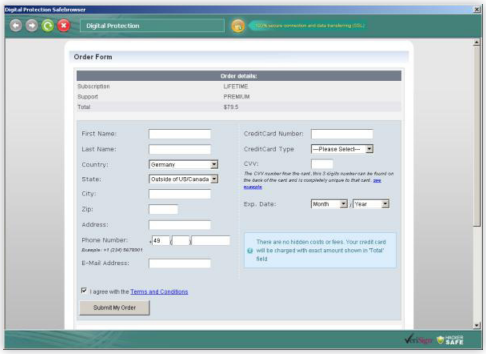


We accept:

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

Fig.28



Digital Protection Safebrowser
Digital Protection
100% secure connection and data transferring (SSL)
VeriSign
HACKER SAFE

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 ( )
Example: +1 (234) 5678901
E-Mail Address:

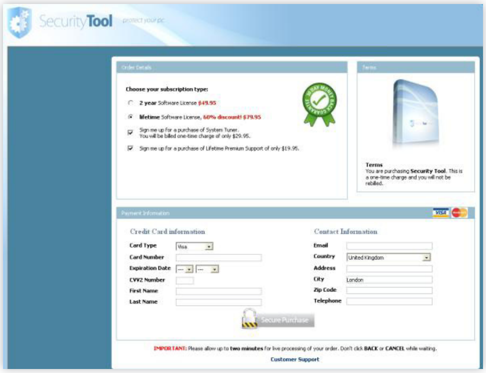
CreditCard Number:
CreditCard Type —Please Select—
CVV:
The CVV number fow the card. this 3 digits number can be found on the back of the card and is completely unique to that card. see example
Exp. Date: Month / Year

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.29



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.

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

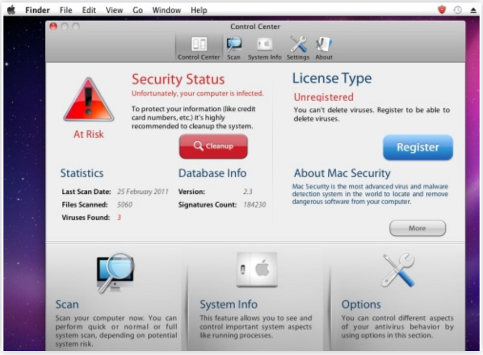
Contact Information
Email
Country United Kingdom
Address
City London
Zip Code
Telephone

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.30



Security Status
Unfortunately, your computer is infected.
To protect your information (like credit card numbers, etc.) it's highly recommended to cleanup the system.
At Risk
Cleanup

License Type
Unregistered
You can't delete viruses. Register to be able to delete viruses.
Register

Statistics
Last Scan Date: 25 February 2011
Files Scanned: 5060
Viruses Found: 3

Database Info
Version: 2.3
Signatures Count: 184230

About Mac Security
Mac Security is the most advanced virus and malware detection system in the world to locate and remove dangerous software from your computer.
More

Scan
Scan your computer now. You can perform quick or normal or full system scan, depending on potential system risk.

System Info
This feature allows you to see and control important system aspects like running processes.

Options
You can control different aspects of your antivirus behavior by using options in this section.

Fig.31

Other fake antivirus behavior

Certain fake antivirus 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 fake antivirus, with a warning message being displayed instead (see fig. 32, 33).

  The fake antivirus 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 fake antivirus families will redirect web requests for legitimate websites 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 fake antivirus (see fig.34).

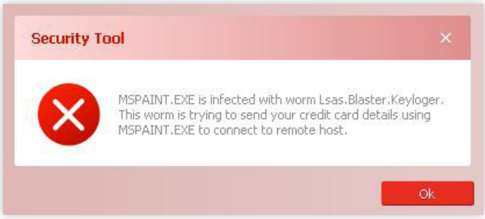
- Installation of more malware: Fake antivirus has been known to download other types of malware upon installation, such as banking Trojans, rootkits and spam bots.

Prevent and protect

There are many ways to stop fake antivirus—on the web, in email, and in your endpoint security. Malware is complex, and protecting the corporate IT environment is a full-time job. Antivirus software is just the beginning. A solid defense is needed to reduce the risk to your business by protecting all routes of attack.

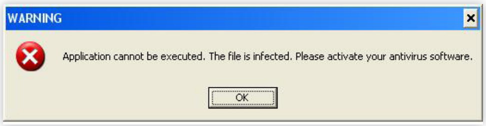
The most effective defense against the fake antivirus threat is a comprehensive, layered security solution. Detection can and should take place at each stage of the infection.

- Reduce the attack surface
- Protect everywhere
- Stop the attack
- Keep people working
- Educate users


Security Tool

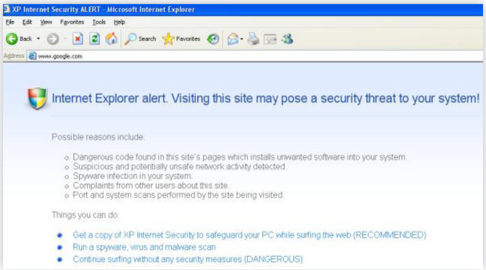
MSPAINT.EXE is infected with worm Lsas.Blaster.Keyloger. This worm is trying to send your credit card details using MSPAINT.EXE to connect to remote host.

Fig.32


WARNING

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

Fig.33


XP Internet Security ALERT - Microsoft Internet Explorer

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)

Fig.34

Here's how you can create this type of layered defense:

Reduce the attack surface – To reduce the attack surface, Sophos filters URLs and blocks spam to prevent fake antivirus from reaching users. By blocking the domains and URLs from which fake antivirus is downloaded, the infection can be prevented from ever happening. Sophos customers are protected by URL filtering in Sophos Web Security and Control19 and the latest endpoint security product. Sophos Email Security and Data Protection blocks spam containing fake antivirus before a user even sees it[20].

Protect everywhere – But, protection needs to go further, and Sophos does this with endpoint web protection, live protection and firewall protection. Sophos Endpoint Security and Control detects web-based content, including the detection of the JavaScript and HTML used on fake antivirus and fake codec web pages. Detection at this layer prevents the fake antivirus files from being downloaded (e.g., Mal/FakeAVJs, Mal/VidHtml).

In addition, Sophos Live Protection enables the Sophos Endpoint Security and Control product to query SophosLabs directly when it encounters a suspicious file in order to determine whether the file is fake antivirus, or any other malware. This enables the automatic blocking of new and emerging malware outbreaks in real time, before the malware has a chance to run. This immediate access lets you close the window between the time SophosLabs finds out about an attack and when users are protected.

Firewall protection means that the Sophos Client Firewall can be configured to block outgoing connections from unknown programs to prevent fake antivirus from "calling home" to receive updated downloads, or to send back a victim's credit card information.

Stop the attack – Stopping the attack involves your anti-malware software, ongoing updating and patching efforts, and run-time detection. To proactively detect the fake antivirus file, our Sophos antivirus agent delivers complete protection, plus low-impact scans that detect malware, adware, suspicious files and behavior, and unauthorized software. Using Behavioral Genotype technology, many thousands of fake antivirus files 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.

Of course, updating and patching are also important to keep anti-malware software up to date, and apply at all levels of protection. Antivirus software must be kept up to date using automatic updating to ensure that the latest protection is provided at all times. Other software such as the operating system and commonly used applications, for example Adobe Reader, should be patched to ensure that they do not introduce security weaknesses. Static defenses are not going to keep up with the new variations, attacks change all the time. So, it is important to allow updates and apply patches as they are received.

Run-time detection is important because if a fake antivirus executable manages to evade the other layers of protection, the Sophos Host Intrusion Prevention System (HIPS) can detect and block the behavior of the fake antivirus sample when it tries to execute on the system[21]. HIPS includes rules that specifically target fake antivirus. Essentially, if the program sees the fake antivirus software doing anything dangerous, it will shut the software down—a blocking move by another layer of protection.

Keep people working – Your users don't really care too much about any of this. They just want to get their work done. That's why Sophos provides IT staff with visibility into fake antivirus detection, sends alerts to let you know when malware has been stopped, and removes the malware from your users' computers. You can choose a configuration that lets users get these notifications, or shows these messages only to the security team.

Educate users – User education is an important part of the defense as well. Users should know not to click on anything suspicious. But, they should also be reminded that the IT department takes care of antivirus protection for their computers. If they are concerned about antivirus, or have strange messages popping up, they should contact IT and not try to sort it out for themselves. It's also important to religiously refuse any anti-malware software which offers a free scan but forces you to pay for cleanup. Reputable brands don't do this—an antivirus evaluation should let you try out detection and disinfection before you buy.

Stopping Fake Anti-Virus

Complete protection against a rampant threat

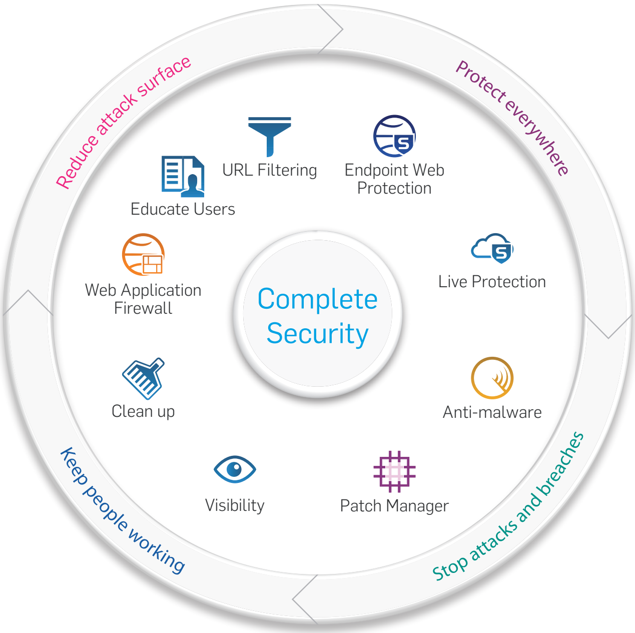


Fig.35

Here are three additional tips to help protect Mac users:

- If you use Safari, turn off the open "safe" files after downloading option. This stops files such as the ZIP-based installers favored by scareware authors from running automatically if you accidentally click their links.
- Don't rely on Apple's built-in XProtect malware detector. It's better than nothing, but it only detects viruses using basic techniques, and under a limited set of conditions. For example, malware on a USB key would go unnoticed, as would malware already on your Mac. And it only updates once in 24 hours, which probably isn't enough anymore.
- Install genuine antivirus software. Ironically, the Apple App Store is a bad place to look—any antivirus sold via the App Store is required by Apple's rules to exclude the kernel-based filtering component (known as a real-time or on-access scanner) needed for reliable virus prevention.

Conclusion

Fake antivirus is still a prevalent threat, it is a persistent problem and the financial benefits for cybercriminals means that fake antivirus will not go away.

Fake antivirus 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 fake antivirus 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. "Fake antivirus Uses False 'Microsoft Security Updates'" SophosLabs blog, http://www.sophos.com/blogs/sophoslabs/?p=8564
3. "Free fake antivirus 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. "Fake antivirus 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 Email Security and Data Protection http://www.sophos.com/products/enterprise/email/security-and-control/
21. Sophos HIPS http://www.sophos.com/security/sophoslabs/sophos-hips/index.html

United Kingdom Sales:
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales:
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Boston, USA | Oxford, UK

SOPHOS