SOPHOS

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 fraudulentlyreported "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 partners¹. 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 Updates²
- Fake Virus-Total pages³
- Fake Facebook app⁴
- ▶ 9/11 scams⁵

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).





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 detected⁶ (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



Fig.6

nthritus Scanter 3	dvanced Security Center			uses. Malware and other thready 🧏
threads hause Son stands Son stands Son stands Son Solid Son Solid Solid	ither Security Tools Individus Scanner Lettings	Feet scan of the most	hypical places where viruses store their files. This scan does no	t take much time and is good for everyday use.
		Scan started; Scan duration; Objects scarry	wd: 9 12:57:49 00:00:13 ad: 252611	pu.cm

- 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.



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 techniques⁸. 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).

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

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).

Edit View History Bookmarks Tools Help

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 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 Rill Look Like File Format: PDF/Adobe Acrobat ... Lcom/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

Harry Wappler Ir

M http://scanweb .net/?p=WKmimHVmaGqHjsblo22EeYVe0KCf2l

1 3 Ahalloween costume pumpki... 3 Online Antispyware Scanner 3 44 V

Fig.10

Latest He

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 ·

4 + · 6 3 😭	http://www1.suaguardprotect08p.	p=p52dcWptaF%2	FCj8bYbn2AeVik
Most Visited - Getting S	tarted 🔂 Latest Headlines 🗸		
🛃 johnny maest 😆 🚷 joe bi	den f bo 😆 👌 treat her like 😆 👌 mich	ael john 🖬 🐫	volcano icela 🧯
System Tasks (8)	System folders	2	
Add or remove programs Change a settings	Shared Documents	My Documents	
Other Places (*)	Mard drive (Ci)		
My Network Places	Security		
Control Panel	Windows Security		
Details (R)	Checking: C_\LocalService\Local Settings\Te	3%	
My Computer	Checking: CA(LocalSerVice)Local Settings(Te	mporary internet rise	es/apvacm.dii
System Folder	Your Computer is infected	0	WARNING 3
	Name	Type	Threat levels
	V Trojan.Thuxemelinf W32.Fujacks.CElinf	Virus Virus	Medium Medium
	Recommend: Click "Start Protection" button	to erase all threats	Start Protection

ধ halloween frankenstei... 😦 💫 Online Antispyware Sc... 😰 🕍 Windows Enterprise S... 😰 🐻 Online Antispyware Sc... paper bag craft halloween frankenstein pumpkin - free video!

~ C

D

Fig.13

arks Tools Help

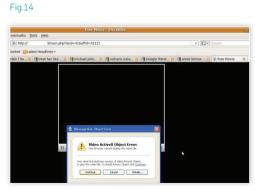
~ 0.

pKDb2yalfaTU2NFfl2dcZoTfn%2BHodiSbr





e i i i i i i i i i i i i i i i i i i i		Security Threat A	malysis - Shiretoko
File Edit View Hig	ory <u>B</u> ookmarks <u>T</u> ools <u>H</u> elp		
+ + - 6 0	1 http://www2.bumvirusnow36.	\?p=p52dcWptaF%	2FCj8bYbn2AeVik12qbVp%
🛅 Most Visited 🗸 🌘 G	etting Started 📓 Latest Headlines 🗸		
👌 johnny maest 😆	👌 joe biden f bo 😆 🛂 treat her like 😆	🛃 michael john 😆	🛃 volcano icela 😆 🔮
Documents Pictures Values Music Pictures Recently Changed Searches Public Public	Vindows Security Vindows Protection Disabled	Local Disk (D:)	
	Threat Name	Threat type	Threat Level
	Trojan. Bankpatch. D Backdoor.Tidserv. K Backdoor.Win32.Haxdoor.gu W32.Daprosy Backdoor.Tidserv Becammended: Click "Frase infected"	Virus Virus Virus Virus Virus Virus	Medium Critical High Critical High



8 min 46 sec, Raiting 9/10, 148541 views ** If the video is not playing please <u>click here</u> to install flash if you don't have it

Fig.12

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 Talk¹⁰. 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 Dear Customer,

Fig.16

You have received an eCard

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

Hey <aim38 .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.

From: "support myspace" <support@myspace.com>

Thanks, The Myspace Team.

Fig.18

Date: 2010-04-19 08:20:46 PST

From: "greetingcard.org" <support@greetingcard.org>

DHL Delivery Problem NR.79631

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.

From: "DHL Manager Susan Murphy" «company@dhl.c

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/JSRedir¹¹.

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 Waled¹⁴. The infamous Conficker worm was also observed to install fake antivirus onto infected computers¹⁵. 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 UAC¹⁶ 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 nonexistent 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).



Check for the latest updates from Windows Update Get support for security-related Change the way Security Center alerts me Scan type: Quick scan Fig.23





Fig.20

🜔 Virus Pr

Quick scan





Fig.21

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 Bulletin¹⁷ and West Coast Labs¹⁸ (see fig.26-31).

					URE	
	\$49	Payment Ty	ment Informatio pe: Credit Card ber ed	n:		
	Your Name and	Address:				
	* First Name		* Country			
	* Last Name		* Zp			
	* Email		* City			
	Phone		* Street			
FRIFIED	Artista				X CLOSE	

Outer family Bundersing ULETING	000	Digital Protection	🚺 🗿 CENtrinten survention auf data barakerug (SC.)	
Decorption URTING Statistic VERSE Total VERS Over Statistic Conditional Random Conditional Random Conditional Random		Order Form		-
Baper Pipelik Test Stands Castolical Stands Hert Stands Castolical Stands Let Function Castolical Stands State Castolical Stands Divert Castolical Stands				
Text B123 First Name: Conditional Structure Conditional Structure Conditional Structure Constructure Conditional Structure Structure Conditional Structure				
First Name: Credit/cell Starbier Lick Name: Credit/cell Starbier Country: First Name: Starb: Creation of Difficulty Starb: Creation of Difficulty Op: Difficulty Address: Difficulty Address: Difficulty Provide Starbier Difficulty Address: Difficulty Provide Starbier Difficulty Starbier: Difficulty Difficulty Difficulty				
Leaf lands: Country : Country :		Total	475.5	
Country: [Vernary] District: [Collard of COC works] District: [Collard		First Name	CreditCard Number:	
Construction of the Construction Construction of the Construction Construction of the Construction Constructin Constructin Construction Construction Constructio		Last Name:	CreditCard TypePlease Select-	
Staffs: [Content AUCCrash] Image and build and an analysis you and in during any analysis of the staff and analysis of the staff an		Country: Germany		
City Dig., Certis Worth Different City Dig., Certis Worth Different City Differen		State: Outside of UDICa	mada It the bask of the card and is completely onique to that card. are	
Adverse: Adverse: Prover Anabes: Adverse: Prover Anabes: Adverse: Prover Anabes: Prover Anabes: Prover Adverse: Prover Adverse		City:		
Prove Rushies		Zip:	thip. Date: North)/Year	
Anamo + 17 2016 Million		Address:		4
E-Mail Address:		Phone Number:	There are no hidden costs or fees. Your credit card	
E-Mail Address:		Risephe +1 (234) 5478011		
		E-Mail Address:	field	
		_		
Submit My Order		P I agree with the Terms and Conditions		
		Submit My Order		



XP Defender Pro New XP Defender Pro XP Defender Pro thing of the past. 1 Year License - \$59.5 2 Years Lie XP Def Identity protect J. Art Our Anti-virus and anti-spyware - safe computer Our Anti-virus and Anti-spyware technology protects you from falling with to which include the second anti-spyware technology matching access of information irewall - block ? and the nok fan ograms in my "39" D ave ever been compo der Pro, While a sing fender Pro gotte close as they called niks for making Defer virus can be in their the net possible Keven Krant. © 2010 XP Defender Pro Technologies Homepage | Buy Now | Support

	÷	0	n
-	IC	.7	ы



Fig.30



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).

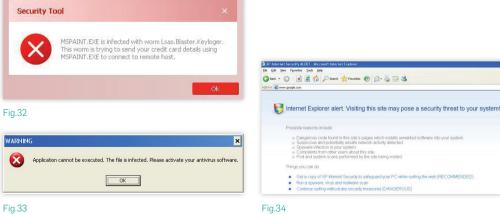
Installation of more malware: Fake antivirus has been known to download other types of malware upon installation, such as banking Trojans, rootkits and spam bots.

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





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 it²⁰.

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.

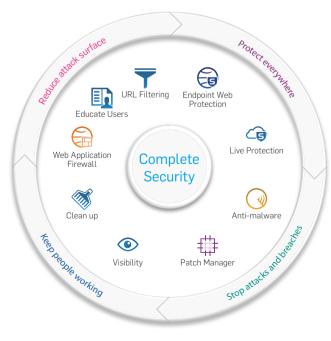
Run-time detection is important because if a fake antivirus executable manages to evade the other layers of protection, the Sophos Host Intrusion Prevention System (HIPS) can detect and block the behavior of the fake antivirus sample when it tries to execute on the system²¹. HIPS includes rules that 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



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 ZIPbased 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 kernelbased 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.

Sophos EndUser Protection Get a Free Trial

References

- "The Partnerka What is it, and why should you care?" Sophos technical paper, http://www.sophos.com/ security/technical-papers/samosseiko-vb2009-paper. html
- "Fake antivirus Uses False 'Microsoft Security Updates'" SophosLabs blog, http://www.sophos.com/blogs/ sophoslabs/?p=8564
- "Free fake antivirus at Virus-Total (That's not VirusTotal)" SophosLabs blog, http://www.sophos.com/blogs/ sophoslabs/?p=8885
- "Phantom app risk used to bait scareware trap" The Register, http://www.theregister.co.uk/2010/01/27/ facebook_scareware_scam
- "Scareware scammers exploit 9/11" Sophos blog, http:// www.sophos.com/blogs/gc/g/2009/09/11/scarewarescammers-exploit-911
- "Fake antivirus Generates Own Fake Malware" SophosLabs blog, http://www.sophos.com/blogs/ sophoslabs/?p=6377
- "Mal/FakeVirPk-A" Sophos security analysis, http://www. sophos.com/security/analyses/viruses-and-spyware/ malfakevirpka.html
- "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
- "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/scarewaretraversing-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-andcontrol/
- 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 Australia & New Zealand Sales: Tel: +61 2 9409 9100 Email: sales@sophos.com.au Asia Sales: Tel : +65 62244168 Email : salesasia@sophos.com

Boston, USA | Oxford, UK © Copyright 2013. Sophos Ltd. All rights reserved. All trademarks are the property of their respective owners. A Sophos Whitepaper 2.13v1.dNA

SOPHOS