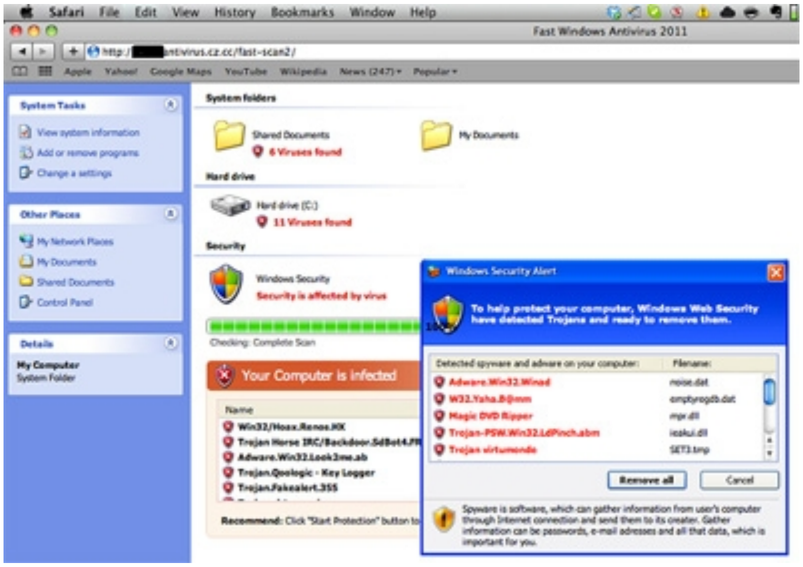
Subject: New Fake Virus on the Mac
From: Terry Rowe <roweterry@fhda.edu>
Date: Wed, 04 May 2011 10:21:26 -0700
To: LUCIW SHARON T <luciwsharon@fhda.edu>, vandercook John <vandercookjohn@fhda.edu>
CC: barretocarlos@fhda.edu, BALIGUAT VICTOR L <baliguatvictor@fhda.edu>, CHEDID KAM M <chedidkam@fhda.edu>, trandavid@fhda.edu, lushan@fhda.edu, MATHIR YUSUF A <mathiryusuf@fhda.edu>, winnkim@fhda.edu, HOLLINS WILBERT E <hollinswilbert@fhda.edu>, PARAGAS BERNIE B <paragasbernie@fhda.edu>, tranlong@fhda.edu, "Max J. Gilleland" <gillelandmax@fhda.edu>

Sharon:
We saw our first Mac "virus" yesterday.
The malware we saw was the one refered to in the article below.
It opened a window in a browser that was very similar to a known pc virus and downloaded a file called "bestmacantivirus2011.mkpg.dmg". In order to be "infected" by this virus, the end user has to install the program which then redirects the user's browser to inappropriate websites and tries to convince the user that they need to pay $29.95 to remove the "virus". In reality, there is no virus - it is a scam to collect money from naive users. Removing the program removes the problem.

Rogueware campaign targeting Mac users

When doing searches the user can be redirected to a malicious domain which checks for: browser agent (it must be Safari), the IP address (only US domains now) and the referrer (if it is Google or other search engine). After these checks the malicious page will show a fake scan screen:



Fast Windows Antivirus 2011

http://[redacted]ntivirus.cz.cc/fast-scan2/

Shared Documents
6 Viruses found

My Documents

Hard drive (C:)
11 Viruses found

Windows Security
Security is affected by virus

Checking: Complete Scan

Your Computer is infected

Name
Win32/Hoax.Renos.HX
Trojan Horse IRC/Backdoor.SdBot4.FR
Adware.Win32.Look2me.ab
Trojan.Qoologic - Key Logger
Trojan.Fakealert.355

Recommend: Click "Start Protection" button to

Windows Security Alert

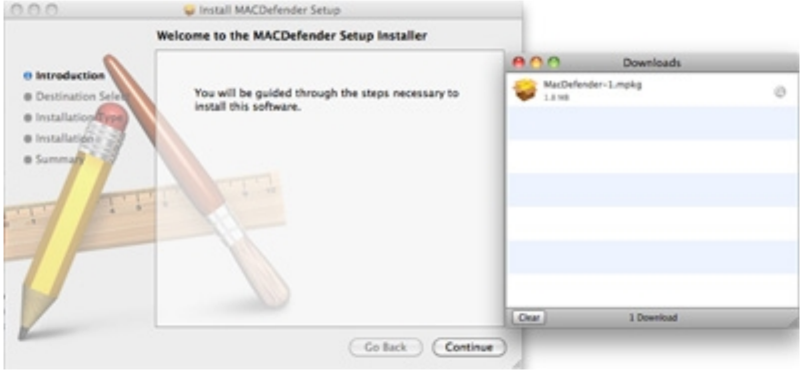
To help protect your computer, Windows Web Security have detected Trojans and ready to remove them.

Detected spyware and adware on your computer:	Filename:
Adware.Win32.Winad	noise.dat
W32.Yaha.B@mm	emptyregdb.dat
Magic DVD Ripper	mpr.dll
Trojan-PSW.Win32.LdPinch.abm	icqkui.dll
Trojan virtumonde	SET3.tmp

Spyware is software, which can gather information from user's computer through 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.

Even though the page is showing a fake Windows screen, the file offered will be a .mpkg:

the installer of the rogue application:

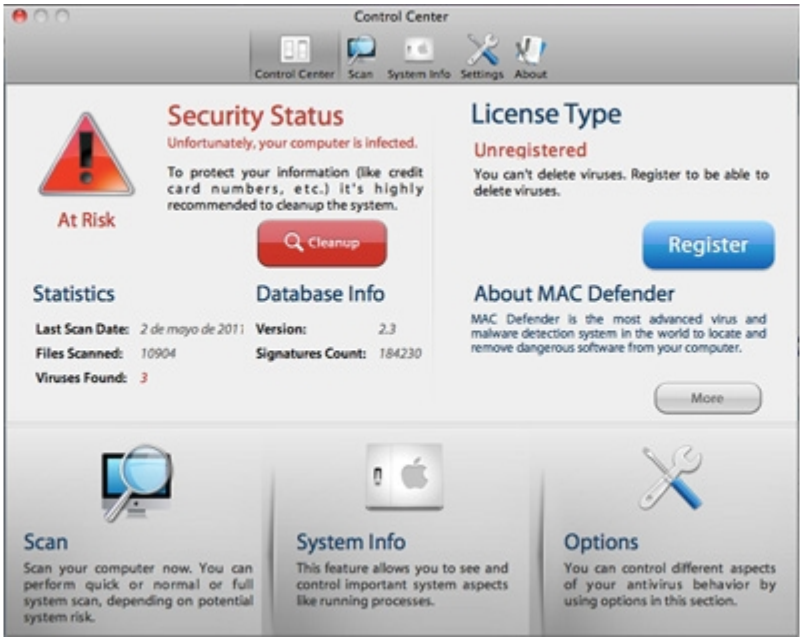


Welcome to the MACDefender Setup Installer

You will be guided through the steps necessary to install this software.

For the application to be installed, the user needs to input his root password.

This is the main window of the rogue application:



Security Status

Unfortunately, your computer is infected.

To protect your information (like credit card numbers, etc.) it's highly recommended to cleanup the system.

License Type

Unregistered

You can't delete viruses. Register to be able to delete viruses.

Statistics

Last Scan Date: 2 de mayo de 2011

Files Scanned: 10904

Viruses Found: 3

Database Info

Version: 2.3

Signatures Count: 184230

About MAC Defender

MAC Defender is the most advanced virus and malware detection system in the world to locate and remove dangerous software from your computer.

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.

http://www.net-security.org/malware_news.php?id=1709

Facebook

247 Twitter 105 Stumbleupon Share 352

- 10 Comments
- Email
- Print

Today @ PCWorld

Fake "MacDefender" Brings Malware to Macs

By Jared Newman, PCWorld   May 2, 2011 12:20 PM

Fake anti-virus software is an old breed of malware that's finally found a new trick: Attacking Macs.

The malicious Mac app is called MacDefender, and according to Intego, it hides within Web pages that use search engine optimization to spam the results of popular searches. Infected Websites show a fake animation of a malware scan in Windows, followed by a pop-up telling users that their computer is infected. JavaScript on the page then automatically downloads a compressed ZIP file containing the malware.

The MacDefender malware looks real.For Safari users who've checked the "open 'safe' files after downloading" option within the browser's settings, the MacDefender malware installation begins automatically. Otherwise, the user must open the ZIP file and install the app manually for the malware to take hold.

The MacDefender installation page.As Intego notes, the MacDefender app--not to be confused with the software developer of the same name--looks rather convincing, and once installed, it quickly sets to work on discovering non-existent viruses and loading pornography in the user's Web browser. The point of all this is to scare users into forking over their money and credit card information, which the MacDefender app says is necessary to delete viruses.

Low Risk So Far

Fortunately, Intego describes this Mac malware as low risk and not very widespread for now. It's also fairly easy to remove, as The Next Web points out. First, use the Activity Monitor (under Applications > Utilities) to disable anything related to MacDefender. Then, make sure there are no references to the malware app in Library/StartupItems or, in the same place, LaunchAgents and LaunchDaemons. Then, move the MacDefender app from Applications to Trash, and delete the trash. Finally, use Spotlight Search to find and delete any remaining references to the app.

For prevention, Intego recommends its own anti-virus software (of course), but all you really need is common sense. Uncheck the "open 'safe' files after downloading" option in Safari and never, ever install anti-virus software that pops up on some random website, no matter how many viruses it says your computer has.
http://www.pcworld.com/article/226846/fake_macdefender_brings_malware_to_macs.html

Terry Rowe
Technical Services Coordinator De Anza College
Foothill - De Anza Community College District
(408) 864-5506
roweterry@fhda.edu