

Conficker: The Latest

The fear of Conficker has brought the first freeloaders to the Conficker scene. Cyber criminals try to sell alleged removal tools for the Conficker worm. According to F-Secure, a Google or other search engine query for Conficker removal tools will produce dubious offers that deliver nothing, and may even infect the PC with malware themselves. The freeloaders generally belong to the scareware developer crowd. They create programs which try to scare users into buying ineffective anti-virus software by displaying false virus alerts on PCs.



Virus-free Conficker removal tools can be downloaded free of charge directly from the sites of several anti-virus vendors. Some of the vendors offering these tools are listed below. The Url (web address) will start the download when typed in the Address Bar of your browser.

Symantec - FixDwndp.exe

http://www.symantec.com/content/en/us/global/removal_tool/threat_writeups/FixDwndp.exe

McAfee - S.T.I.N.G.E.R.exe

http://vil.nai.com/vil/conficker_stinger/S.T.I.N.G.E.R.exe

Trend Micro - SysClean-WORM_DOWNAD.zip

https://securecloud.com/downloads/SysClean-WORM_DOWNAD.zip

Kaspersky - KKillerv3.4.3.zip

<http://data2.kaspersky.com:8080/special/KKillerv3.4.3.zip>

Side Note

In early 2009, hackers penetrated a web server, from where they were able to work their way further into FAA systems and were able to gain access to the personal details of 48,000 current and former FAA employees. In other cases, intruders were able to obtain an administrator password and use it to install their own applications on West coast air traffic domain controllers. In 2006, a virus even forced the FAA to shut down a portion of its air traffic control systems in Alaska.

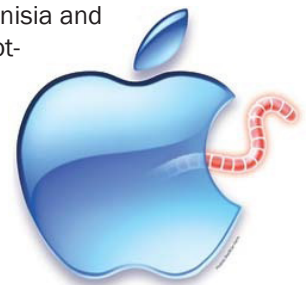
For all our MAC using friends

Virus writers have created a worm that seeks to establish a botnet of compromised Mac machines. But the Tored Mac worm, which attempts to spread via email, is so hopelessly buggy and lame that it's about as likely to score as Steve Ballmer at an Apple convention.

Strains of Mac malware are, of course, dwarfed by factors that run into the hundreds of thousands, if not millions, by types of Windows-specific viruses. The small, although growing, number of Mac malware strains that do exist are typically Trojans that pose as video codecs or pirated versions of iWork. Such Trojans commonly frequent multimedia websites (actually run by hackers) or P2P networks.

Tored takes a different approach towards attacking Mac fans - but that's one of the few factors in its favour. Net security firm Sophos explains that Tored is an email-aware worm which attempts to harvest email addresses from Mac machines it infects, before forwarding copies of itself to those targeted accounts.

The malware was created in Tunisia and aims to be the first Mac OS X botnet agent, according to comments in the source code of the malware.



Except a Mac-specific Trojan discovered in April has a better claim to the title "first Mac OS X botnet agent". Furthermore Tored is riddled with so many mistakes it's incapable of doing any harm, Sophos reports.

"Bugs in the worm's code, however, mean it is unlikely that you will ever encounter it, even if the author had taken the time to correct the many spelling mistakes in the emails it tries to send," writes Graham Cluley, a senior technology consultant at Sophos.

The author of the code has adopted a novel approach in order to encourage its spread, or just to apologise for inconveniencing Windows and Linux users. A message in the code reads:

For Mac OS X ! :(If you are not on Mac please transfer this mail to a Mac and sorry for our fault :)

Firefox

Unless you're a Firefox power user, you may not be familiar with the about:config page. The Firefox about:config page is not so much a page as it is a somewhat hidden configuration section. It's hidden because it's fairly powerful and not nearly as simple to use as the standard Preferences window. In the about:config page, you have to know what you are doing or you can mess things up a bit. In fact, when you attempt to go to that page for the first time, you have to accept an agreement (which is really just a warning) before you can continue.

How this page works is simple. You reach the page by entering about:config in the address bar. There are entries (one per line) that handle various types of configurations. Each entry has a searchable keyword. The entries can be of Boolean, integer, or string value. Entries contain Name, Status, Type, and Value. Typically, you will be modifying only the Value, by double-clicking on it and making the change. With all of that in mind, let's take a look at 10 of the best ways you can "hack" the about:config page.

Tips for advanced users

If Firefox is fubar'd because you accidentally misconfigured about:config, you can fix it in one of two ways: Make a backup of your prefs.js file before you start editing. Then, if something goes wrong, you can restore it by copying it over the corrupt file.

If you can't restore via a backup prefs.js file, you can exit Firefox and issue the command `firefox -safe-mode` to bring up the Firefox Safe Mode screen. Then, just select Reset All User Preferences To Firefox Defaults. Note: This will restore all user preferences to their default values.

If you are uncomfortable, or unsure about doing this DON'T.

1: Speed up Firefox

This hack requires a few steps. Search for pipelining in the filter and you should see:

network.http.pipelining: Change this to true.
network.http.proxy.pipelining: Change this to true.
network.http.pipelining.maxrequests: Change this to 8.

Now search for max-connections and you should see:
network.http.max-connections: Change this to 96.
network.http.max-connections-per-server: Change to 32.

2: Disable antivirus scanning

This is only for the Windows version. If you're downloading large files, this scanning can seriously slow things down. And since you will most likely scan the downloaded file anyway, you'll probably want to disable this. Of course, if you are uber paranoid (not a bad trait for computing), you might want to leave this entry alone.

To disable antivirus scanning, search for scanWhenDone and you should see:

browser.download.manager.scanWhenDone: Change this to false.

3: Open Javascript popups as tabs

If a popup window lacks the features of a browser window, Firefox will handle it like a popup. If you would prefer to open all windows, including popups, as new tabs, you need to tell Firefox in about:config. Search for newwindow and you will see three entries. Of those three entries, you will want to modify:

browser.link.open_newwindow.restriction: Change this to 0.

4: Spell check in all fields

By default, Firefox checks spelling only in multiple-line text boxes. You can set it to check spelling in all text boxes. Search for spellcheckdefault and you should see:

layout.spellcheckDefault: Change this to 2.

5: Open search bar results in new tab

When you use the search bar, the results display in the current tab. This can be a nuisance because you will navigate out of the page you're currently in. To make sure Firefox always opens search results in a new tab, search for openintab and you should see:

browser.search.openintab: Change this to true.

6 Auto-export bookmarks

In Firefox 3, bookmarks are automatically saved and exported for you. The only problem is that by default, they're saved as places.sqlite instead of the more convenient bookmarks.html. To change this setting so that they can be easily re-imported, search for autoExportHTML and you should see:

browser.bookmarks.autoExportHTML: Change this to true.

