

Last-minute Conficker survival guide [1]

Tomorrow -- April 1 -- is D-Day for Conficker, as whatever nasty payload it's packing is currently set to activate. What happens come midnight is a mystery: Will it turn the millions of infected computers into spam-sending zombie robots? Or will it start capturing everything you type -- passwords, credit card numbers, etc. -- and send that information back to its masters?

No one knows, but we'll probably find out soon.

Or not. As Slate notes, Conficker is scheduled to go "live" on April 1, but whoever's controlling it could choose not to wreak havoc but instead do absolutely nothing, waiting for a time when there's less heat. They can do this because the way Conficker is designed is extremely clever: Rather than containing a list of specific, static instructions, Conficker reaches out to the web to receive updated marching orders via a huge list of websites it creates. Conficker.C -- the latest bad boy -- will start checking 50,000 different semi-randomly-generated sites a day looking for instructions, so there's no way to shut down all of them. If just one of those sites goes live with legitimate instructions, Conficker keeps on trucking.

Conficker's a nasty little worm that takes serious efforts to bypass your security defenses, but you aren't without some tools in your arsenal to protect yourself.

Your first step should be the tools you already have: Windows Update, to make sure your computer is fully patched, and your current antivirus software, to make sure anything that slips through the cracks is caught.

But if Conficker's already on your machine, it may bypass certain subsystems and updating Windows and your antivirus at this point may not work. If you are worried about anything being amiss -- try booting into Safe Mode, which Conficker prevents, to check -- you should run a specialized tool to get rid of Conficker.

Microsoft offers a web-based scanner (note that some users have reported it crashed their machines; I had no trouble with it), so you might try one of these downloadable options instead: Symantec's Conficker (aka Downadup) tool, Trend Micro's Cleanup Engine, or Malwarebytes. Conficker may prevent your machine from accessing any of these websites, so you may have to download these tools from a known non-infected computer if you need them. Follow the instructions given on each site to run them successfully. (Also note: None of these tools should harm your computer if you don't have Conficker.)

As a final safety note, all users -- whether they're worried about an infection or know for sure they're clean -- are also wise to make a full data backup today.

What won't work? Turning your PC off tonight and back on on April 2 will not protect you from the worm (sorry to the dozens of people who wrote me asking if this would do the trick). Changing the date on your PC will likely have no helpful effect, either. And yes, Macs are immune this time out.

Source URL: <http://www.aspira.org/en/last-minute-conficker-survival-guide>

Links:

[1] <http://www.aspira.org/en/last-minute-conficker-survival-guide>



To empower the Puerto Rican
and Latino community through
advocacy and the education and leadership
development of its youth.

Last-minute Conficker survival guide

Published on The ASPIRA Association (<http://www.aspira.org>)
