

Home

Subscriptions & Memberships

Contact

About eJSS

System Safety Society



Vol. 45, No. 3 • May-June 2009



## Confound That Conficker!

by Sherry R. Deatrack

Pages 1 | 2

### Tech Corner

Download printable PDF of this page

We're all careful about not clicking on links in suspect Web sites. We don't open emails from strangers. You might think that only networked computers are at risk, but new computer worms, viruses and Trojan horses are getting so sophisticated, you may not even know that your home computer is being recruited to join a malicious botnet. What's a typical computer user to do?

It's easy to succumb to the FUD (fear, uncertainty, doubt) being spread about. Conflicting reports abound. Some said April 1, 2009 was to be Armageddon day for the PC when Conficker C kicked into action. Others said if you take sensible precautions, your computer would probably emerge unscathed.

Most people have heard of the Conficker virus by now. The original version of Conficker reared its head on November 20, 2008. Conficker has undergone several variations since its inception. Conficker B arose in December, and in early February, 2009, became B++, which was able to download software, giving its creators greater freedom to use infected computers. As of this writing, the latest variant is Conficker C. Previously infected computers miraculously started updating from the B variant to the C by means of a new dynamically linked library (DLL) that is suspected to have come through Conficker's Internet rendezvous point mechanism and began spreading on March 4, 2009.

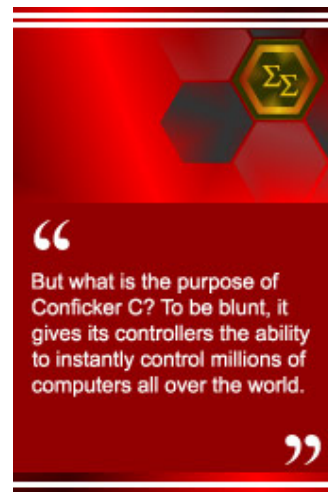
This third iteration is a major restructuring, adding a new peer-to-peer (P2P) coordination channel, and a revised domain generation algorithm. It cloaks its functions under a layer of code that hinders analysis. Very clever, and very vicious.

Conficker spreads by exploiting a Windows loophole to attack networked computers. But it can also spread by USB devices (cameras, iPods, portable drives, etc.). More than 10 million computers are alleged to have been infected by Conficker as of February, 2009.

The infected machines could be used to send spam or log keystrokes in addition to the denial-of-service attacks. Thanks to a group known as the Conficker Cabal, the worm has been kept in check so far, by cracking the algorithm the B++ version uses to find rendezvous points on the Internet where it gets new code. See [www.hostexploit.com](http://www.hostexploit.com) for more information on tracking the Conficker (also known as "Downadup") worm.

In response to the Conficker Cabal's blocking of the worm's domain registration points, Conficker C arose. Now, it uses points taken from a pool of more than 50,000 randomly generated domain name candidates each day. This poses a major challenge to the Cabal.

Conficker C cloaks its presence on the host computer. Thus, even an attentive user won't notice it. It then deletes all restore points prior to its infection so you can't go back to the time before C appeared. It also sets NTFS file permissions on its stored file image to prevent write and delete privileges. Every time it begins, Conficker C starts a thread to disable security services and terminate Conficker removal software. This thread also disables Windows services that deliver security patches and software updates. If you have set your computer to automatically update Windows software, Conficker simply won't allow it. If you've had trouble getting updates for your Windows programs, chances are, your computer is a victim of Conficker.



### Safety Training

offered by A-P-T Research, Inc.

#### Courses

Principles of System Safety Engineering

Software System Safety Engineering

Safety Assessment for Explosives Risk (SAFER)

Institute of Makers of Explosives Safety Analysis for Risk (IMESAFR)

Explosive Safety Training

#### Technical Information

Melissa Emery, (256) 327-3396

#### Registration Information

(256) 327-3399  
training@apt-research.com

#### Safety Engineering and Analysis Center



4950 Research Drive  
Huntsville, AL 35805  
[www.apt-research.com](http://www.apt-research.com)

President's Message

From the Editor's Desk

TBD

In the Spotlight:

Considering System Risks

Redundancy for Safety

Gains from Losses:

System Safety and Aging Systems

Tech Corner

Chapter News

Mark Your Calendar

About this Journal

Classifieds

Advertising in eJSS

Contact Us

Puzzle

Who is responsible for the Conficker worm? No one knows for sure. Researchers at the University of Michigan are busy tracking down the first victim in hopes of finding out where it came from, using darknet sensors gathering more than 50 terabytes of data from all over the world. The U.S. Department of Homeland Security is funding this activity. CNET reports that BKIS, a Vietnamese security firm that makes the BKAV antivirus software, has found evidence that the worm originated in China, rather than in Russia or Europe, as was previously rumored. BKIS bases its conclusion on a similarity in code to 2001's Nimda virus (no one, however, has verified that Nimda originated in China). Chinese analysts dispute this assertion, claiming it is politically motivated.

But what is the purpose of Conficker C? To be blunt, it gives its controllers the ability to instantly control millions of computers all over the world. It keeps other worms from uploading anything to the Conficker "drone" or "zombie" computers, giving these criminals a virtually indestructible army of computing power. The implications of such control are staggering. Imagine how quickly the economy would collapse if suddenly all bank transfers stopped. An army of 10 million networked computers is greater than those used in a denial-of-service attack that brought down Estonian government computers. A large Internet site, such as Google or Amazon for instance, could easily be brought down or blackmailed by such a large botnet. A bank account (or all of a bank's accounts) could be emptied overnight, resulting in worldwide panic.

On the other hand, Dean Turner, director of Global Intelligence Network Symantec Security Response, says we should relax. "The sky is definitely not falling," says Turner. Hmm...that's reassuring! Experts say the worm has stopped propagating, and that tools exist to remove it from computers. These experts say that Conficker C has infected the fewest number of computers. What's strange is that the B variant is not set to a particular date, yet hasn't done anything malicious so far. Turner thinks the worm's creators have stopped spreading it because they have enough infected machines to suit their purpose, whatever it is.

[next page »](#)

Home

Subscriptions & Memberships

Contact

About eJSS

System Safety Society



Vol. 45, No. 3 • May-June 2009

Focus

## Confound That Conficker!

Download printable PDF of this page

by Sherry R. Deatruck

Pages 1 | 2

Another security researcher, Joe Stewart from SecureWorks, is confident that no meltdown will happen. He says all that will occur is "the worm will begin to use a new trick that gives it a better chance of getting around existing defenses that attempt to prevent it from updating." Your hard drive is probably safe, according to Stewart. Modern malware authors aren't mere pranksters, so destroying your hard drive is pointless to them. Let's face it — profit is their motive. They wouldn't be able to enlist your computer in their zombie botnet if they destroy your hard drive.

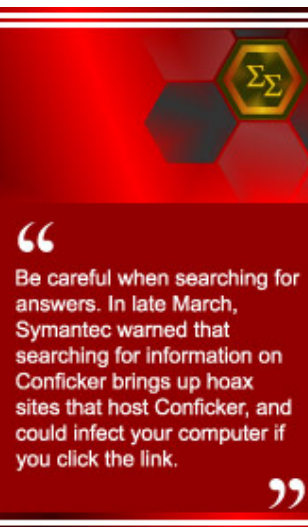
Conficker C isn't the only worm in town. In fact, Symantec reports that 2008 was the worst year on record for malware. Known malware has increased during the last 12 months from tens of thousands to more than 600,000 new original and variant codes. It's downright scary. One such worm, the "psybOt," has corralled more than 100,000 computers, using home routers and DSL modems, including Linksys routers. This botnet performs distributed denial-of-service attacks, which makes an Internet site or service unavailable to its intended users. These attacks are most often aimed at banks and credit card payment gateways by flooding the target with so many communication requests that it can't respond to legitimate traffic. This botnet can also gather personal information and passwords from your computer. DroneBL, a real-time IP tracker that scans for botnets and vulnerable machines, says psybOt is hard to detect on a home computer and it can disable access to your router's controls, making a factory reset the only way to clear this worm.

Some Internet bots are ostensibly non-malicious. FreeRice.com is a Web site that relies on advertisers to sponsor its rice donation program through the United Nations World Food Program. It has a word game, and for each correct answer you give, they donate 10 grains of rice to people in need. Once it became well known, some people created scripts to play the game automatically, 24 hours a day. One script caused a donation of more than three million grains of rice in a few hours. By contrast, when I played the game, I was able to make a donation of 300 grains of rice in 10 minutes or so. While these scripts' creators have a noble purpose, they might unintentionally cause the advertisers to abandon the site, since real people aren't reading the ads.

What can you do to protect yourself from malware? The possibilities are endless, and I've only scratched the surface here, but here's some sound advice I found on a techno-geek discussion board called LansingOnline.com. According to "Artie See" (I don't know if that's his real name), "running Zone Alarm personal firewall, Avast anti-virus and Ad-Aware anti-spyware together is a very good effective combination to protect your computer." He goes on to suggest that you make sure your programs, virus signature files, and spyware signature files are all up to date. He suggests using the automatic update feature. And whatever you do, never open any attachment you're not completely sure is safe. You wouldn't have unprotected sex with strangers, would you? (You don't have to answer that.)

If you want to quickly check for infection, go to a site like f-secure.com, secureworks.com or microsoft.com. If your computer says, "Page cannot be displayed," Conficker is probably blocking your access.

What do you do if your computer is infected? See says, "A two-way firewall like Zone Alarm will alert you if a malicious



### 27th International System Safety Conference

#### Commemorative Coins



Accepting Advance Orders Now

#### Registration

2 Aug 09, 1-5 pm CST,  
3 Aug 09, 7 am

#### Meet & Greet

Embassy Suites Lobby  
2 Aug 09, 5:30-7:00 pm

#### Opening Ceremonies & Keynote Speakers

3 Aug 09, 9:00 am



Visit [ISSC2009.org](http://ISSC2009.org) for frequent updates.  
Visit our sponsors' websites.

- President's Message
- From the Editor's Desk
- TBD
- In the Spotlight:
  - Considering System Risks
  - Redundancy for Safety
- Gains from Losses:
  - System Safety and Aging Systems
- Tech Corner
- Chapter News
- Mark Your Calendar
- About this Journal
- Classifieds
- Advertising in eJSS
- Contact Us
- Puzzle

program is trying to 'phone home' (XP's built-in firewall checks incoming data only, not outgoing). And if there is ever any doubt, you can simply disconnect from the Internet until you are sure."

See goes on to say, "In my opinion, Zone Alarm is the most powerful and most effective personal firewall program available, and you can't beat the price (free). Either Avast or AVG are excellent free choices for anti-virus. And Ad-Aware from Lavasoft is one of the two best anti-spyware programs, the other being Spybot from Safer Networking Ltd." See subscribes to Spy Sweeper by Webroot.

Be careful when searching for answers. In late March, Symantec warned that searching for information on Conficker brings up hoax sites that host Conficker, and could infect your computer if you click the link. And watch out for those fake virus warnings that try to trick you into buying a program to "clean" your computer. Use free programs like "SpyBot Search and Destroy" and "MalwareBytes" to get rid of these fake warnings. Windows Defender is a good choice if you use Windows XP.

It's tricky navigating the Internet these days. The answer might be, as some of my computer geek friends suggest, to just stop using Windows. They all use Apple Macs or use Linux with Ubuntu. You can go to <https://help.ubuntu.com/community/LiveCD> to get a free disk that contains two versions of the Linux OS — a full-install copy and a version that will run on top of Windows. I haven't tried these yet, but I'm on the verge of switching. You can't be too careful.

---

Fight back against the Conficker worm and other malware:

- Microsoft Malicious Software Removal Tool — <http://www.microsoft.com/security/malwareremove/default.aspx>
- F-Secure removal utility — <ftp://193.110.109.53/anti-virus/tools/beta/f-downadup.zip>
- McAfee's detection tool — <http://www.mcafee.com/us/enterprise/confickertest.html>
- Latest Windows software update — <http://update.microsoft.com>
- Get a free PC Safety Scan — <http://onecare.live.com/site/en-us/default.htm>
- Read about how to protect yourself from Conficker — <http://www.microsoft.com/protect/computer/viruses/worms/conficker.msp>
- Check to see if your PC is part of a botnet — RUBotted (Beta) from Trend Micro, or BotHunter from SRI International

If you're really industrious, you might earn the \$250,000 reward Microsoft has offered for information leading to the arrest and conviction of the Conficker creators. Call the Antivirus Reward Hotline at 425-706-1111, or email your tips to the Antivirus Reward Mailbox, [avreward@microsoft.com](mailto:avreward@microsoft.com). Whatever you do, surf wisely and avoid the shark-infested waters.

[« previous page](#)