

Wednesday, March 25, 2009

# Cybersheriffs arm selves for Conficker showdown

## Computer worm may slither out on April 1

By Byron Acohido  
USA TODAY

SEATTLE — In the brief, tumultuous history of cybercrime, there has never been anything quite like the Conficker worm.

In the past few months, Conficker's creators have infected at least 3 million Windows PCs worldwide with malicious software, and perhaps as many as 12 million. At this moment, the bad guys are locked in a high-stakes showdown with a posse of security groups led by Microsoft.

Conficker's controllers have set a date for what amounts to a cyber-shootout at the OK Corral. Next Wednesday — April Fools' Day — millions of infected PCs, called bots, will begin reporting for further instructions, presumably to begin spreading spam, stealing data or carrying out online scams. And there appears to be little the good guys can do to cut off such communications.

"We have not yet begun to feel the real impact of Conficker," says Paul Henry, researcher at security firm Lumenion. "We may soon be at the whim of those in control of what has emerged as a formidable army of infected machines."

### Vintage worm

Conficker requires no action on the part of the PC user to spread. It's a throwback to self-replicating worms that scanned the Internet for PCs displaying known — and unpatched — Windows security holes.

Such worms largely disappeared after 2004, as Microsoft improved its process for identifying new holes and quickly issuing patches. But last September, Chinese hackers began selling a \$37.80 program for tapping into a newly discovered Windows hole on some 800 million machines worldwide, according to SRI International, a non-profit research firm.

Microsoft took notice, and on Oct. 23, issued a rare emergency patch. Most home PC users in North America got patched quickly, via Windows Auto update. But many corporate and govern-

ment users were lackadaisical about patching. In China and other nations where pirated copies of Windows are widely used, patches simply weren't available. "Once the patch was out, no one paid attention," says Don Jackson, senior researcher at SecureWorks. "They underestimated the risk."

Precursors of Conficker began spreading on a limited basis, mostly in Asia. In early January, a full-featured version began seeking out unpatched PCs across the globe. The worm slithered onto any shared hard drives; it searched out nearby servers and issued hundreds of combinations of user IDs and passwords to break in; it copied itself onto any device plugged into a USB port, such as thumb drives, music players or digital cameras. When that infected device later got inserted into another work station, that machine became infected.

Conficker also took extraordinary measures to prevent each new bot from being disinfecting by Microsoft or antivirus programs, or usurped by a rival botnet group. SRI found, for instance, that Conficker's encryption algorithm came

from MIT's Ron Rivest, copied from a recently published research paper.

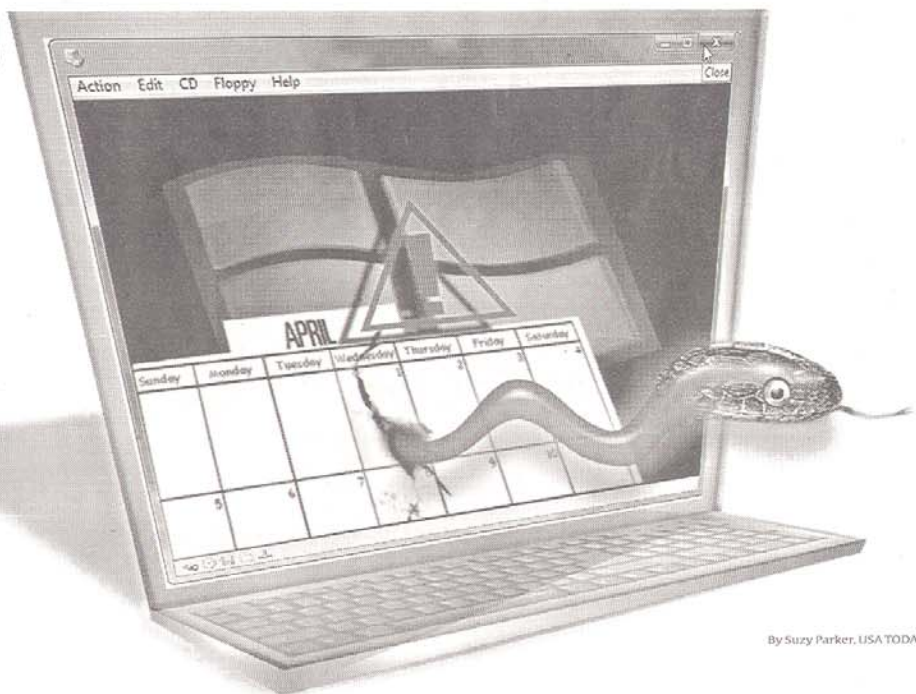
On Feb. 12, Microsoft put up a \$250,000 bounty for information leading to the capture of Conficker's creators. The software giant also formed an alliance of security groups, dubbed the Conficker Cabal, to battle the worm.

The Cabal focused on disrupting what was perhaps Conficker's most unnerving feature. Eight times a day, each bot tried to connect with a list of 250 randomly generated Web addresses — each a potential rendezvous point to receive further instructions. Each day, this list of 250 rendezvous points changed.

To cut this off, the Cabal identified the Web addresses scheduled to turn up on the daily lists, and began registering any that weren't already registered by someone else. The goal: to "pre-empt registration of those domains for potential criminal use," says Christopher Budd, of Microsoft's security response team.

### Upgrade slips through

Yet, on March 6 and on March 17, the



By Suzy Parker, USA TODAY

### Repelling Conficker

Several tools can detect and block malicious programs. Here are three:

- ▶ **WinPatrol ([www.winpatrol.com](http://www.winpatrol.com))**. This free tool, long popular with techies, blocks and alerts you to any malicious program that tries to install itself on your hard drive. WinPatrol Plus, designed for consumers, costs \$30 for a lifetime subscription.
- ▶ **BufferZone Pro ([www.trustware.com](http://www.trustware.com))**. This tool sends all Internet traffic to a virtual buffer zone, stopping any malicious program from running on your hard drive. Cost is \$40 for an annual subscription, with a free one-month trial now available.
- ▶ **Enigma SpyHunter ([www.enigmaoftware.com](http://www.enigmaoftware.com))**. This anti-spyware supplier has produced a free tool designed specifically to inspect for, and remove, Conficker infections.

bad guys somehow slipped a malicious software upgrade to millions of infected PCs. The upgrade began organizing the bots into a vast peer-to-peer, or P2P, network, says SRI program manager Phillip Porras. P2P networks are powerful and flexible, because each PC can function as a command server. They're commonly used to share videos and music and play complex online games.

The upgrade also included instructions for each bot to begin a daily routine on April 1 of checking in at 500 rendezvous points, randomly selected from a pool of 50,000 domain names. This trick will make it more difficult for the Cabal to preregister addresses, says Porras.

Joe Stewart, a senior researcher at SecureWorks, notes that the infected PCs are already capable of receiving directives from the controllers via the P2P network, "so the 50,000 domains aren't really needed. They could even be a practical joke on the part of the authors."

Botnets have emerged as the cybercrime world's tool of choice to carry out scams. Josu Franco, Panda Security's director of business development, surmises that Conficker's controllers may be moving methodically to corner the market on botnets for hire. "This is free inventory for them," says Franco.

The good guys' defense boils down to vigilance. While the Cabal may not be able to stop the controllers from issuing directives, it remains poised to disrupt any criminal activity attempted by Conficker bots.

"There may be a second phase of the threat at some point in time," acknowledges Microsoft's Budd. "However, we believe, given the tremendous amount of attention this worm has received, industry and law enforcement efforts will be a deterrent to a large second wave of attacks."