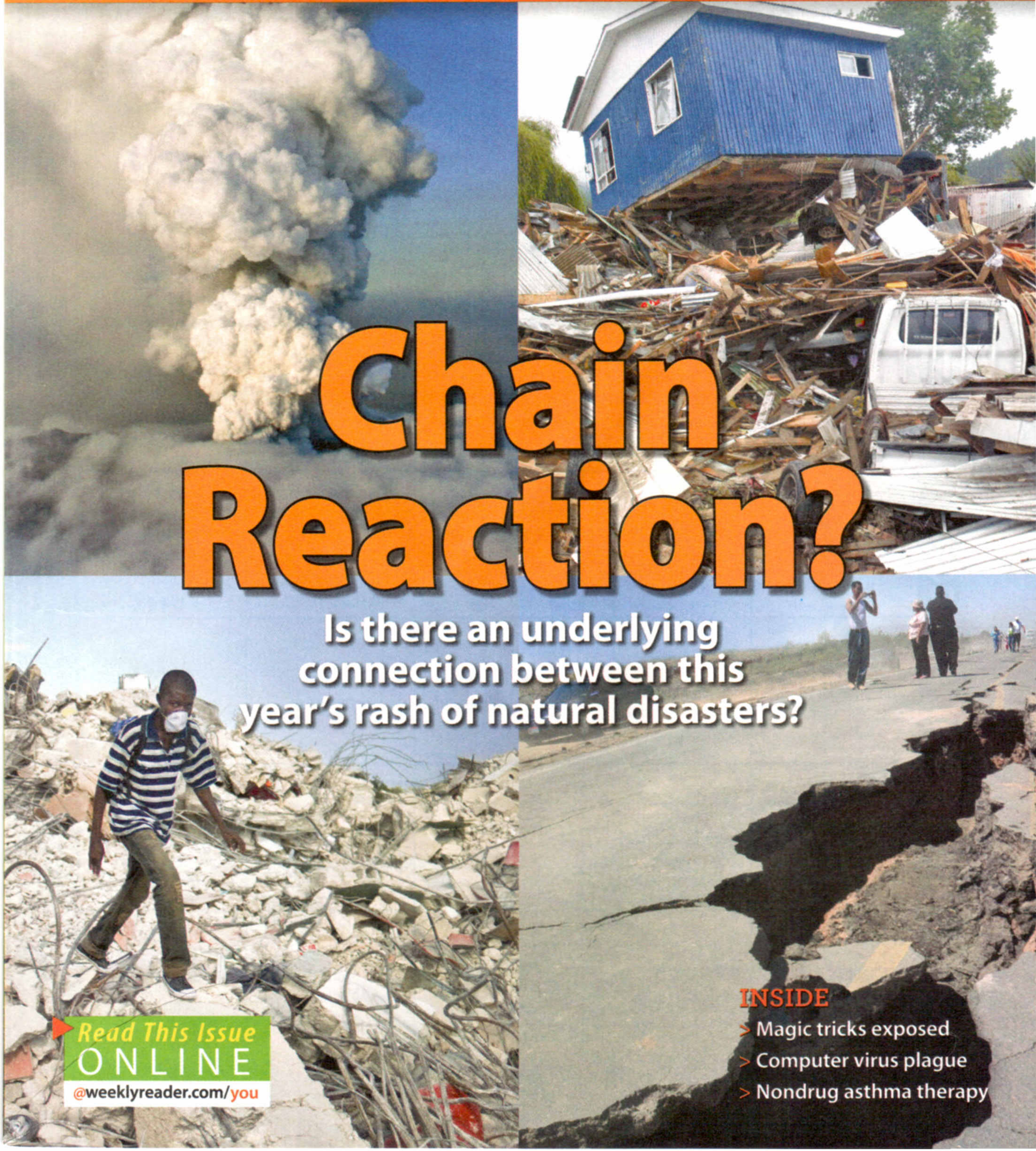
Weekly Reader

current science®

SEPT. 17, 2010

VOL. 96

ISSUE 2



Chain Reaction?

Is there an underlying connection between this year's rash of natural disasters?

INSIDE

> Magic tricks exposed

> Computer virus plague

> Nondrug asthma therapy

Read This Issue ONLINE

@weeklyreader.com/you

A potentially dangerous computer program is spreading around the world, and NO ONE KNOWS HOW TO STOP IT.

On Nov. 20, 2008, the honeypot at SRI International trapped a new foreign agent. Twenty-one minutes later, it trapped the same agent again. And so it went, over and over in the ensuing hours and days.

"It seemed that [the agent] had bloomed overnight and was attacking from every country on the Internet," Phil Porras, program director of SRI's Computer Science Laboratory, told *Current Science*. SRI is a nonprofit institute that conducts research and development for governments and businesses.

A honeypot is a computer designed by security experts to lure malicious computer programs that travel around the Internet. The honeypot that Porras operates has trapped thousands of those malicious programs, known as *malware*, over the years. But the one it snared that November day was unlike any seen before.

Almost two years after that malware burst on the scene and spread like the plague, computer experts are still engaged in a frantic game of catch-me-if-you-can. They're trying to keep it from wreaking havoc one day through a vast network of zombie computers.

COMPUTER INFECTIONS

Computer malware comes in three varieties: *viruses*, *Trojans*, and *worms*.

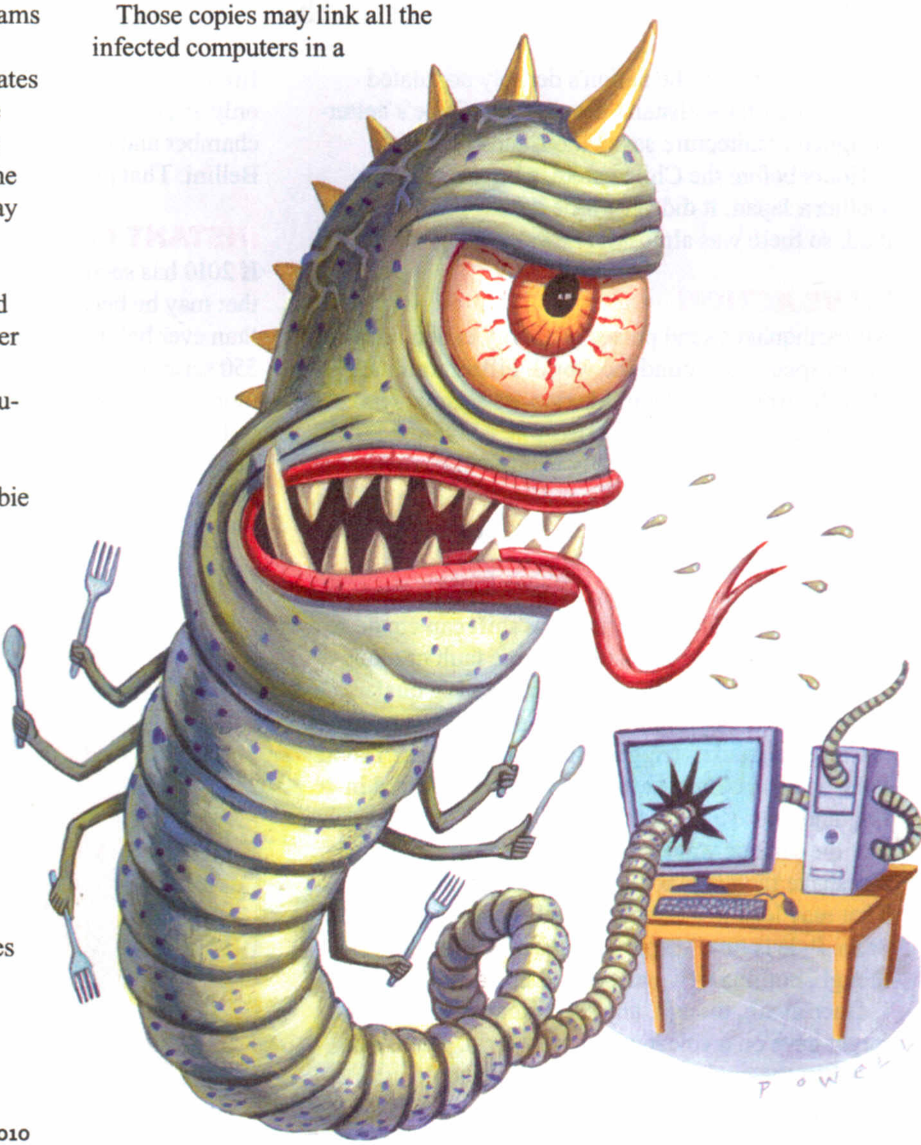
- A virus is a small program that piggybacks on another program. Each time the main program runs, the virus runs too. The virus might *replicate* (make copies of) itself and attach those copies to other programs. Or it might wreak havoc by, say, deleting files or causing a computer to crash frequently.

Some viruses are attachments to e-mail messages. "Never open e-mails from strangers," advises Porras.

- A Trojan is a program that appears to do one thing. It may claim to be a game, for example. When you run it, though, it attacks the computer.
- A worm is a program that sneaks into a computer through a hole in its security system. It replicates and then sends the copies to other computers through the same hole.

Those copies may link all the infected computers in a network—a *botnet*. Many botnets exist today, each one linking thousands or tens of thousands of computers.

The worm that entered SRI's honeypot on November 20 replicated so quickly and spread so widely that other security outfits immediately took notice too. They gave the worm names such as Kido and Downadup, but the label that held was Conficker. A worldwide web of computer security experts now tracking the worm calls itself the Conficker Cabal.



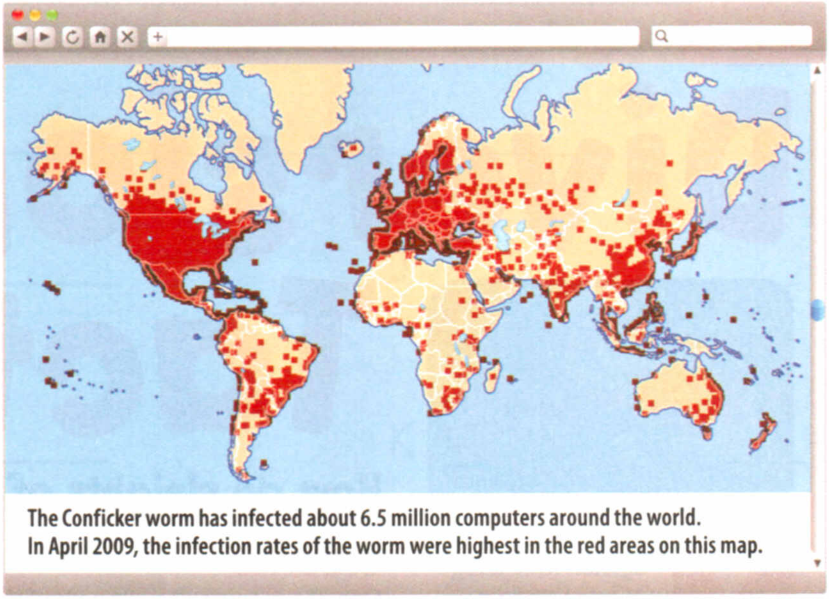
SOFT SPOTS

Like all worms, the Conficker worm infected computers through vulnerable spots in their operating systems. A computer's operating system has thousands of *ports*—gateways to other computers through which data is sent and received. A *firewall* is a security system that protects those ports.

On Oct. 23, 2008, the Microsoft Corporation issued a bulletin to all Microsoft users. The bulletin identified a port—Port 445—that wasn't protected by a computer's firewall at certain moments, making computers vulnerable to worms. The bulletin warned users about the problem and told them how to *patch* (repair) it.

A month later, the Conficker worm invaded computers through Port 445. Some security experts speculate that the worm's creators took advantage of the October 23 bulletin to identify a port through which the worm could enter. How could a worm invade a port that users had already been warned about and told how to patch? Because many users ignore Microsoft's bulletins, and many other users own *bootlegged* (illegally copied) versions of Microsoft programs and don't receive the bulletins.

Since the appearance of the Conficker worm, the Conficker Cabal has been engaged in an all-out effort to quash it—to stop it from spreading, to locate its command center, and to decode communications between the command center and the botnet. The cabal has watched dumbfounded as the worm has mutated in response to every leap in progress it has made. The worm now resides in an estimated 6.5 million computers, giving no clue to its presence but chatting quietly with every other copy. Clearly, the worm's creators are a team of diabolically clever people, educated in every facet of computer science.



The Conficker worm has infected about 6.5 million computers around the world. In April 2009, the infection rates of the worm were highest in the red areas on this map.

Computer worm illustration by Charlie Powell; Computer screen: Shutterstock; Map: Joe LeMonnier

CRUEL INTENTIONS?

Who are those creators? One clue to their identities may have surfaced in the original version of the worm. It held instructions to infect computers everywhere in the world except the eastern European country of Ukraine. Eastern Europe has many highly skilled computer scientists.

If the creators' identities are unknown, what about their intentions? Some computer scientists think the worm is simply a pawn in a mischievous game of cat and mouse. Others believe something more fiendish is afoot. Eastern Europe has many well-organized criminal gangs. The worm has already damaged some hospital and military computer systems. If it infiltrates one of the United States' major cyber networks—telephone or banking or air traffic control, for example—its command center could instruct it to bring down the whole thing, says Porras.

Meanwhile, the worm continues mutating, replicating, and spreading. Says Porras: "The potential for one country or terrorist group to use the [Conficker worm] to buy access to the computers of another country's critical infrastructure, government, or military is a real and constant danger." **CS**

Worm Infestation

By Hugh Westrup