

California Computer Care

News,
Views,
Tips and
Cool Techniques
for CCC Members

March 2004
Vol. VII, No. 3

We
speak
Geek,
so you
don't
have to.

Why I'm glad to be a Mac User reason number 1278

Here's a newspaper article that I couldn't resist reprinting. This is from the *Knight Ridder Newspaper* syndicate, 3/6/2004. By Erika D. Smith.

World domination begins at home.

Maybe even at your home if you're one of the millions of computer users surfing the Web without protection. The virus writers know you're out there—and they're fighting for you.

For weeks, three groups of malcontents have been waging a cyberwar with different versions of the MyDoom, Bagle and Netsky e-mail viruses.

It started out as friendly—if annoying—competition, with one virus writer trying to outdo his rivals by releasing a more powerful computer bug onto the Web.

But now it's personal.

Insults have been exchanged. Dares have been made. Attacks have been launched. And the stakes, well, they're higher than ever.

The goal, some say, is global control of an army of infected computers. Those Internet-connected minions could then be told to send out more tainted e-mail or spam—and where there's spam, there's money.

“There's definitely a war going on, and unfortunately, the casualties are the AV (anti-virus) industry and Internet users,” said Steven Sundermeier, a vice president at Medina, Ohio-based Central Command Inc.

No one knows who the virus writers are.

Some say they're hired guns working for professional spammers.

Others believe they're just publicity hungry teenagers.

Either way, the war has antivirus software programmers running around like geeks looking for caffeine. Like a vide-

ogame recluse exposed to the sunlight. Like . . . well, you get the idea.

Joe Hartmann of Trend Micro Inc. said he was up until 5 a.m. Wednesday putting out the latest fire in an unusually long stretch of outbreaks.

“It seems like every other day we're seeing a new variant” of MyDoom, Bagle or Netsky, he said.

Things really heated up Friday, when the authors of Bagle released a third version of the virus, or variant. C. Bagle is now up to variant K, successfully spreading around the world despite the release of a cure.

Over the same five days, Netsky's authors created three new versions of their virus. Netsky's apparent agenda is to disable Bagle and MyDoom. Every time a computer is infected with a new version of Netsky, the virus erases any trace of Bagle and MyDoom, effectively stealing control of the PC.

The authors of MyDoom have responded by releasing MyDoom.G, a variant that is not disabled by Netsky.

And just in case there was any misunderstanding about the virus writers' intent, they've started leaving notes for each other.

The authors of Bagle.J wrote in the programming code: “Hey, NetSky, (expletive) off you (expletive), don't wine our business, wanna start a war?” Netsky's writers retorted: “Skynet AntiVirus—Bagle—you are a loser!!!!” and “We are the skynet—you can't hide yourself!—we kill malware—MyDoom.F is a thief of our idea!”

Juvenile insults aside, Central Command's Sundermeier isn't convinced that the authors of these viruses are amateurs.

Neither is John R. Levine, the author

of *Internet for Dummies* and *Fighting Spam for Dummies*.

“Back in the good old days, virus writers were teenagers with no social lives,” he said. “But about a year and a half ago, spammers started hiring professional virus writers to send out spam.”

These days, spammers and virus writers work together like *Pinky & the Brain*. Most junk e-mail carries some sort of virus. As many as 10,000 new spam-related infections are reported a day, Levine said.

Spam is big business, with some people making six figures selling mortgages and “bodypart enlargement” pills.

“The margins are enormous and why not? Unhappy customers aren’t willing to complain to the cops,” Levine said. “What are they going to say? I bought some Viagra that didn’t work.”

Hartmann disagrees that spammers are behind the MyDoom-Bagle-Netsky plot to take over the world’s computers. It’s probably just a spitting match between warring programmers, and it even could be one person trying to cover up his tracks.

“Most virus writers get really excited about what they did.” said Hartmann, who is director of North American research for No. 3 antivirus provider Trend Micro. “Most of them are kids.”

No matter how many mad scientists are behind the curtain, there are only a few ways to demolish the MyDooms of the world. Levine said it’s not going to be through antivirus software.

“No amount of beating up on users is going to get them to update their antivirus programs because they don’t care,” he said.

Internet service providers need to cut off customers with infected PCs until they fix them.

“It’s really easy to tell because they go from sending four e-mails a day to sending like 400,” he said. “Nobody makes friends that fast.”

Antivirus companies hope it doesn’t come to that. In the meantime, Sundermeier urged everyone not to open unexpected e-mail attachments, and to buy, install and update their security software.

“Unfortunately, the global fight over superiority may result in a victory for the cybercombatants,” he said, “but

not for the general Internet user population.”

Why am I so glad to be a Mac User? Because this cyberwar between email criminals does not affect us! Our Macs cannot be hijacked by these viruses and used to victimize others. Our Macs are safe from viruses, spyware* and other attacks because they have been designed to be safe. Windows users are victims because Windows is designed to be victimized.

I like our way better.

*Spyware is software that unnoticed, records your every move and reports to unknown third parties. A very common problem in the Windows world.

March Tip—

Back issues of the California Computer Care newsletter have been updated and reformatted for easier reading. You can find back issues on the CCC website:

<http://www.calcompcare.com>

Click on the [News](#) link and choose a year to browse.

CCC newsletter back issues are in PDF format. Mac OS X users can read them with Adobe Reader or the Preview application. For Mac OS 9 use Adobe Acrobat Reader.

California Computer Care

P.O. Box 9445

Santa Rosa, CA 95405

(800) 540-8989

help@calcompcare.com

Like an
auto club
for your
computer.