pressdemocrat.com

SSU expert: Conficker worm is superior to anything he's seen before

By NATHAN HALVERSON
THE PRESS DEMOCRAT

Published: Tuesday, March 31, 2009 at 3:43 a.m.

George Ledin, a professor of computer sciences at Sonoma State University, teaches an advanced course on how to write computer viruses. It is the only such course in the United States, and makers of anti-malware software have criticized Ledin for teaching it.

Press Democrat: How worried should people be about Conficker?

Ledin: People probably have enough to worry about. In Conficker's case, most people can't do much, if anything.

Computer professionals should be worried. There hasn't been anything like Conficker so far. It's a brand new game, with unknown rules.

One good side effect of Conficker might be raising people's consciousness so that malware education and research are not viewed as strange or taboo anymore.

PD: What is so extraordinary about this virus?

Ledin: Well, it's technically a worm, not a virus. I prefer to use "malware" so as to avoid semantic debates. As malware goes, Conficker is superior to any malware seen to date. It is not going to be stopped anytime soon. The worm's author is very knowledgeable about Microsoft Windows internals.

It has not destroyed anything yet, but it has successfully infected millions of computers. It uses a very sophisticated approach to installing and spreading,

and a recent version exploits peer-to-peer technology, which would make any one machine a potential lieutenant in Conficker's army.

Nevertheless, Conficker could incorporate more, better features. It's not stealth -- it does not do advanced rootkit-like tricks to hide its presence (it could take up residence in the kernel and hide from the file system and the list of services executed within the svchost.exe process). Such functionalities would make Conficker much more difficult to detect.

It does not appear to be about money. The botnet could have been raking in money after the Conficker's second revision. Its installed base is large enough for income, and criminals are known for their avarice, not for their restraint.

(Editor's Note: The difference between a virus and a worm is a virus needs to be attached to another file sent by a human, while a worm can spread without any human interaction.)

PD: Who do you think might be behind Conficker?

Ledin: This ought to be a multiple-choice question:

(a) Pimply teenage hacker.

(b) Russian, Ukrainian, Eastern European, Chinese, Brazilian organized cybercriminals.

(c) Rogue government black ops.

(d) Secret U.S. agency scientists.

(e) George Ledin's students.

(f) Some of the above.

(g) All of the above.

(h) None of the above.

In other words, I don't know. I don't know anyone who knows or is willing to tell me. The location, assumed to be abroad, cannot be substantiated either. Maybe Conficker was launched here.

When I asked my students if, instead of pimply teenage hackers, Conficker might be the product of some government's black ops, my students voiced their doubts. My colleague, John Aycock from the University of Calgary, opined that if

it were black ops, its discovery would alone mean failure.

Also, Conficker's activity level is too high: black ops/info warfare-type malware should be very patient, slow and surreptitious. It really ought to be invisible.

PD: What does the general public not know about malware that they really should?

Ledin: Well, where should we start? Not patching Windows vulnerabilities is bad. Using Windows is risky. Visiting sleazy sites is stupid. Relying on anti-virus packages is naive (and useless). Learning as much as possible about malware is prudent.

Malware thrives on ignorance and social engineering, so the more users know the better off they'll be. But Conficker and future worms and viruses keep up and overtake any ordinary user's defenses. We need to support research and education rather than run like Chicken Little all the time.

PD: How do you think your class that teaches students how to write malware will help protect the public?

Ledin: Currently we have an intolerable situation: the bad guys have all the know-how, all the tools. I am committed to educating computer professionals who will help solve the problem. Without the help of many eyes and brains, the malware problem will only get worse.

I've been discussing Conficker with my students. They have the inventiveness, the ingenuity of talented beginners, for whom nothing is impossible, and are not cowed or burdened by the weight of convention.

I am only a professor with a few eager students, working on a shoestring budget. If my students, complete beginners, can so easily bypass all computer defenses, and so cleverly comprehend how malware, such as Conficker, courses through the Internet's veins, just imagine how hundreds of classes like mine would tilt the odds in our direction, the good guys.

This interview was conducted via e-mail by Staff Writer Nathan Halverson, who can be reached at at 521-5494 or nathan.halverson@pressdemocrat.com. Check out his blog at DailyGeek.Pressdemocrat.com or on twitter.com/eWords