Posted: 29/06/2006 | **By:** Jon Boroshok

Social engineering's new tricks present bigger dangers

June 6, otherwise known as 6/6/06, received its proverbial 15 minutes of fame recently, as news reports playfully covered the symbolic Devil's date. Not so coincidentally, the IT world met the underworld of computer security.

The publishing of "A pact with the Devil," Paper TR-666 by the University of Cambridge Computer Laboratory introduced the concept of the "Satan virus," which authors Mike Bond and George Danezis say exploits, "not the incompetence or naivety of users, but instead their own greed, malice and short-sightedness."

The paper alleges that malware can "provide enough incentives to users for them to willingly maintain it on their systems," hence it can be like entering a pact with the devil. The incentives can include some sort of perceived gain of power or information, or a fear of being exposed as retribution for removing the malware.

"The Satan virus is a theoretical proposal to illustrate new design principles that could, in theory, be used, along with more traditional ones, to propagate and entrench computer viruses," said Danezis, now a visiting fellow at K.U. Leuven, Belgium.

Danezis said that using carrot and stick principles, the concept illustrates how viruses can use bribery, such as access to other people's files and free music downloads, or even blackmail its victims to further its spread.

Industry experts offered varying opinions on the paper's worth and validity. David Perry, Global Director of Education for antivirus vendor Trend Micro Inc. in Cupertino, Calif., questioned the seriousness of the paper.

"It's a paper about a theoretical method someone could use to write a virus," said Perry. "There is a long history in academia of joke research papers." He called the paper an elaborate scenario of social engineering.

Patrick Peterson, vice president of technology for email security vendor IronPort Systems Inc. of San Bruno, CA, dubbed it "a hypothetical exploit to propagate viruses," pointing out that it is standard security technique to do experiments to see what works in order to be able to combat it. However, he said he could envision how a program written to harvest connections on social sites like MySpace.com could inflict considerable damage.

Natalie Lambert, a security analyst for Forrester Research Inc. in Cambridge, Mass., said that people do knowingly accept spyware and adware on their computers in order to obtain something they deem valuable.

"As long as the consumer has chosen to install the software (and knows what additional software comes with the application), the spyware is not the issue," Lambert said.

Danezis said there are still many cases in which infected emails with subject lines as simple as "I love you" entice recipients to open them.

"Some viruses these days, when installed, would encrypt valuable files and blackmail users," he said. "This is slightly different from what we discuss [in the research paper], but clearly shows that virus designers are getting up to speed with using bribery and blackmail."

Danezis admitted that the paper's release date was intentional and meant to heighten interest, but the theories discussed are hardly out of the realm of possibility.

"Formulating these principles is a "novel and worthy contribution to the field of computer security and virus research," he said.