Beneficial Malware: Cybernetic Oxymoron

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

Greg Moorer, an undergraduate student in the Department of Computer Science at Mississippi State University, won a Best Student Paper award at the 23rd NISSC for his paper on beneficial computer viruses and worms*. The author reviewed the literature on beneficial viruses, unfortunately including the completely mythical “Iraqi printer virus” (based on an old April Fool’s joke about a virus that crawled out of printer ROMs and up the parallel cable to infect PCs) as an example of a beneficial virus.

Aside from this glitch, the author did an excellent job of summarizing the classic objections of Vesselin Bontchev to using self-replicating code. Bontchev’s arguments include

* the difficulty of controlling viruses once they are released;

* magnification of quality assurance problems when code reproduces;

* platform- and version-incompatibility;

* unauthorized and undocumented modification of data;

* unauthorized an undocumented resource utilization;

* inability of viruses to accomplish any function other than reproduction better than normal programs;

* technical support complications in infected systems;

* danger of Trojan Horse viruses with harmful payloads despite their beneficial description; and

* likelihood that malicious-virus writers would claim that their work was beneficial.

In contrast, Moorer cites the ideas of Fred Cohen, who has argued for years that viruses could do useful things such as compressing files or destroying other viruses. The student then modeled the anti-virus virus concept by using a simulated population of ten users into which he released a virus and then a virus-hunter virus. He found that the anti-virus virus should be constrained in several ways:

* it should be released into the same “discourse community” (i.e., in the same way as the target virus);

*	it must be released from an otherwise virus-free computer;

*	it must have a limited lifetime; and

*	it should remove itself automatically when its expiry date is reached.

My own immediate thoughts are that the state of quality assurance in today’s commercial environment is so abysmally poor that I seriously doubt the wisdom of infecting anyone’s systems with self-replicating code regardless of intent.

The author also chose not to treat the legality of any such system for infection without authorization; any such act might be considered a violation of existing laws on unauthorized entry into computer systems.

Finally, there have been cases of “genetic” exchange between macro viruses; e.g., the “mating” macro viruses of 1997 that exchanged parts of their ASCII payload messages.   Such uncontrolled modifications of self-reproducing code should give any network manager pause before accepting any execution of external code on production systems.

On the other hand, many users feel that receiving automatic updates from trusted sources such as their operating-system vendor or anti-malware supplier is perfectly acceptable.   Perhaps a system of digital certificates would allow those who want to participate in patch distribution via self-reproducing code could reduce their risk to some extent using such a mechanism. Nonetheless, there is a fundamental objection to using certificates as a measure of software quality: knowing the origin of code does not imply knowing the quality or safety of that particular code.

In summary, as a former data-center manager who still waits at least six months for the first Service Packs before installing a new operating system on my own PC, the prospect of having my system infected by unauthorized code intended to help me is distasteful at the least.

* Moorer, G. (2000).   The case for beneficial computer viruses and worms: A student’s perspective.   _Proceedings of the 23rd NISSC_:449.

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>.   He invites inquiries about a wide range of information security courses and INFOSEC consulting services that he and his colleagues at AtomicTangerine would be delighted to deliver to your employees at your site and at your convenience.   For Web-based or CD-ROM online training in security from our INFOSEC University project, see < http://infosecu.com >.

For information about AtomicTangerine, visit < http://www.atomictangerine.com >.

limit on any Web site, and to republish it in any way they see fit.