Was Nimda Virus Part Of Destabilization?

by Fletcher James

There are reasons to suspect that the Nimda computer virus, released one week to the hour after the stunning airplane crashes into the Pentagon and World Trade Center, is a part of the currently ongoing strategic destabilization operation. In my evaluation, as a computer programming specialist of 25 years experience, the development of Nimda required an extensive, multi-disciplinary team of experts. This was no more an amateur exploit, than were the airplane attacks. The following facts are relevant.

- Nimda is the fastest spreading worm ever created. Thirty minutes after its first detection, thousands of computers around the world had picked it up; within 36 hours, an estimated 200,000 machines were infected.
- Due to the speed of its spread, it has been possible to narrow down the time of introduction to between 0800 and 0900 EDT, Sept. 18. This falls within the time frame, projected by Lyndon LaRouche several days earlier, for a possible second wave of destabilization.
- As amply documented in the industry press, Nimda has done more damage than any prior cyber-attack. Although anti-virus vendors were able, within a few hours, to provide "virus signature" files which would recognize and block Nimda, there is currently no way to disinfect a machine that had already been infected, other than to erase all software, and re-load from scratch.

There are several reasons for Nimda's incredible virulence:

- It utilizes several, completely different, technologies for attack—based on, and targetting, multiple platforms. These include:

(a) propagation through e-mail;

(b) searching for, and infecting, files on other computers on the local network;

(c) taking advantage of the same security hole as used by the Code Red virus to locate, probe, and infect Web servers;

(d) taking advantage of an additional "back door" opening which exists on servers which were previously infected by Code Red, and not entirely cleaned up;

(e) passing infection to client computers which simply visit an infected website.

- Although most anti-virus software contains "generic scanners" which analyze incoming code for patterns of programmed activity that indicate possible dangerous actions, and although there are at least five identified modes of propagation, nevertheless not a single generic scanner managed to recognize Nimda code as a potential threat. This would tend to indicate that some form of stealth technology was in use.
- At least one feature of Nimda required an extraordinary hacking job: it can infect a PC whose user is simply viewing an e-mail, without opening any attachments. Hackers have expended hundreds or thousands of *man-years* looking for holes in e-mail systems which would allow them to do this. With all of that effort, there was only one such hole previously found, which was exploited by the Melissa virus last year, and that hole was closed. The ability to infect a PC which is simply browsing a compromised site, is another rare and difficult task.

Not An Amateur Job

These and other facts suggest that this was no amateur job, and was not done by an isolated individual. There are so many different exploits involved in this code, that it would require a team of highly experienced individuals with a wide variety of skills.

For example, I can see only three means to accomplishing the task of infection via e-mail preview: (1) by assigning a large number of highly skilled hackers under central control; (2) by placing operatives into the core of the extended hacker community, and locating someone who had found a hole and was willing to shop it out; or, (3) by penetrating Microsoft Corporation, and either stealing source code (which is known to have happened at least once in the past year) so as to find a security hole, or modifying source code so as to create one.

The hacker community is a swamp, very much akin to the swamps in which other forms of terrorists and proto-terrorists breed. The bulk of the swamp consists of amateurs, whose primary motivation is to play a few pranks and make a name for themselves. These then segue into anarchist circles whose self-perceived motivation is to attack "the system" and sow chaos for its own sake. Finally, there are hard-core intelligence agencies, whose aim ranges from serious industrial espionage, to outright warfare. (Elements of Israeli intelligence, for example, are widely suspected to be included in this category.)

Also, like the other swamps, there are extensive "counter-terror" penetrations of the hacker community, by the FBI and other agencies, with the putative goal of detecting and preventing attacks, and therefore the included capability of aiding that which they are allegedly opposing.

Finally, one must ask the question: Since this was such a polished piece of software, was it ready for release before Sept. 11? If not, then it were unlikely that any team of amateurs could or would concentrate on finishing a project under the circumstances of that week. If, on the other hand, Nimda was ready to go, in advance of Sept. 11, then it was in the hands of an agency whose preparation and timing was designed to intensify such a crisis.