**Network Security**



# Son of MyDoom Stalks Microsoft


By Erika Morphy
Enterprise Security Today
February 10, 2004 1:42PM

**Doomjuice appears to be targeting Microsoft, as did Mydoom.B. Security firm F-Secure reported that Microsoft's Web site experienced a disruption in service on Monday as a result. Such incidents are likely to continue in the foreseeable future, as the new worm has been programmed to start a DoS after February 8th.**

COMPLETE STORY





A major battle may have been won against MyDoom.A, which spread like wildfire earlier this month and last, but the war against this computer worm still rages on. A variant, dubbed "Doomjuice," has appeared on the scene.

Because of the similarity between the Doomjuice and MyDoom codes, it is clear that the same author has written both, Alan Wallace, spokesperson for security company Panda Software, told NewsFactor. "The attacks, in fact, leverage the computers infected by MyDoom.A," he said.

Unlike earlier versions, which counted on tricking unsuspecting users into downloading infected attachments, the new worm exploits an open port, or backdoor, created by MyDoom.A -- in much the same way that Slammer exploited a server vulnerability.

According to Wallace, Doomjuice creates an entry in the Windows Registry (HKEY_LOCAL_MACHINE SOFTWARE Microsoft Windows CurrentVersion Run "Gremlin" intrenat.exe), then generates a copy of itself to launch a denial of service (DoS) attack against Microsoft.

So far this morning, he said, none of Panda Software's clients have been affected. The company issued a patch for Doomjuice yesterday, he noted.

## Setting Its Sights on Microsoft

Doomjuice appears to be targeting Microsoft, as did MyDoom.B. Security firm F-Secure reported that Microsoft's Web site experienced a disruption in service on Monday as a result. Such incidents are likely to continue in the foreseeable future, as the new worm has been

programmed to start a DoS after February 8th.



However, Doomjuice's main goal is not necessarily to shut down Microsoft, Tony Magallanez, a systems engineer with F-Secure, told NewsFactor.

"Doomjuice delivers the source code of the original worm to the infected computer, which is almost never done. Normally, computers that get infected rarely, if ever, have the source code on the hard drive, which makes it much easier to identify the culprits."

But since Doomjuice is implanting the original source code on infected hard drives, it will be much harder for the authorities to convict the virus writer or writers, Magallanez says.



## ABCs of Patch Management

Not that companies needed yet another lesson in the efficiencies of automating patch management internally. However as such attacks become ever more commonplace, it is clear that patch management has moved beyond the status of "best practice" to "mandatory business requirement."

"It is what we do in-house and what we recommend to our clients," Anthony Deighton, general manager of Siebel ERM, told NewsFactor. He noted that there are two schools of thought behind patch management, though: Some companies do not like to automate patch updates because there is always a percentage of computers that break in the process. "Our view is that [the] risk of rolling out a patch that might break a single's person machine is less than the risk of having a virus slip into the network," Deighton said.

Siebel grades the threat as the update comes in, then catalogs all the machines affected by the threat, Deighton said. Not surprisingly, the company uses its own software to manage this process, including cataloging the infrastructure and rolling out data to employees as to the status of their machines and Siebel's response to the situation.

As for Doomjuice, in particular, Siebel probably can relax. This particular variant is attacking mainly home users who have broadband connections and who have not cleaned their computers after the first wave of MyDoom struck, Magallanez said. "It's a slower-moving virus than the earlier ones, but we guestimate that there are tens of thousands infected machines still out there." NF


| Related Stories | Latest News & Special Reports |
|---|---|
| MS Issues Explorer Fix, Girds for MyDoom (3-Feb-04) | PeopleSoft Board Rejects Oracle's Final Offer |
| MyDoom Forces SCO To Change Address (2-Feb-04) | Juniper Buys NetScreen in $3.4B Stock Deal |
| MyDoom Crashes SCO Site (1-Feb-04) | Linux Security on the Ropes |
| MyDoom Mutates, Targets Microsoft (29-Jan-04) | The Secret World of ReiserFS |
| SCO Posts Bounty for MyDoom Creator (28-Jan-04) | ISPs Top Electronic-Billpay List |
| | Son of MyDoom Stalks Microsoft |
| | Mozilla Unveils Firefox Browser |