

DoS worm

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/incidents/2004-10/0039.html>

From: David Gillett (gillettdavid_at_fhda.edu)

Date: 10/20/04

To: <incidents@securityfocus.com>

Date: Wed, 20 Oct 2004 13:48:02 -0700

Yesterday, someone (we believe it was one of our students) unplugged a lab Mac from the campus network and plugged in a PC (laptop, we assume). Besides whatever the user wanted, it apparently did three things:

1. Attempt to open a lot of connections (port 22, SSH) to shaman.exodus.ro (62.80.109.128), then
2. Send a SYN flood, spoofing the source address as 0.0.0.0, to ports 22 and 80 of weed.powered.at (195.149.115.18), and
3. Probe random addresses in our Class B space (port 445, CIFS); if it got a connection, it tried various SMB-type things amongst which I was able to pick out the string "IPC". Five other machines in our space eventually demonstrated similar symptoms.

I don't know what this beast is. I infer that #2 is a DoS attack which is perhaps the purpose of the worm, and that #3 is its spread vector via the IPC\$ share.

Anybody recognize this?

Dave Gillett