

# How Easily Can JetDirect Modules for HP Printers Be Hacked?

---

*Source:* <http://www.derkeiler.com/Newsgroups/comp.security.misc/2007-08/msg00028.html>

---

- *From:* "Will" <[westes-usc@xxxxxxxxxxxxxxxxx](mailto:westes-usc@xxxxxxxxxxxxxxxxx)>
  - *Date:* Wed, 29 Aug 2007 00:30:01 -0700
- 

We have a Laserjet 8100 that has one dedicated JetDirect J3113A module for an internal network and one dedicated JetDirect module for a no man's land. My firewall is picking up the JetDirect module on the no man's land doing nbname (port 137) lookups to public IP addresses owned by county governments. Obviously that isn't good behavior, and it's probably not normal behavior for a JetDirect module to initiate such lookups. I looked at the web interface on the JetDirect, and no configuration page is explaining the behavior I'm seeing.

I'm concluding that either the JetDirect has been hacked, or alternately someone is spoofing its IP (unlikely).

Does anyone have information on how easily a JetDirect can be hacked, and are there particular versions (or configurations) that are more robust from a security standpoint? I am thinking of isolating the shared printers on their own dedicated subnet behind the firewall, to minimize possibility of further infection to other machines, but would like some insight about what I am up against first.

[P.S. sorry for separate post to comp.security, but I had forgotten that group is largely abandoned in favor of this one.]

—  
Will