

## Re: On classifying attacks

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2005-07/0273.html>

---

**From:** Godwin Stewart ([gstewart\\_at\\_spamcop.net](mailto:gstewart_at_spamcop.net))

**Date:** 07/17/05

Date: Sun, 17 Jul 2005 11:41:54 +0200  
To: Derek Martin <[code@pizzashack.org](mailto:code@pizzashack.org)>

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

On Sat, 16 Jul 2005 12:40:29 -0400, Derek Martin <[code@pizzashack.org](mailto:code@pizzashack.org)> wrote:

- > *It seems to me your statement can't be correct, because this is ALWAYS*
- > *the case. A local exploit requires that a local user run an*
- > *executable. A remote exploit requires that a local user run an*
- > *executable, even if that is accomplished merely by booting the system.*
- > *All exploits require running code, and code doesn't magically start*
- > *itself... Running code is required, because it is the very running*
- > *code which is being exploited.*

Maybe so, however with the case of the BIND attack, the vulnerability in locally running code (named) is being exploited by a remote attacker via the network.

In the case of an e-mail containing malicious code, the code being exploited (parts of the Windows kernel or whatever) is being attacked by code running locally - on the \*same\* machine. In this sense it can hardly qualify as a "remote" exploit.

---

G. Stewart - [gstewart@spamcop.net](mailto:gstewart@spamcop.net)

A lot of money is tainted. 'Taint yours and 'taint mine.

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v1.4.1 (GNU/Linux)

iD8DBQFC2ifiK5oiGLo9AcYRASwqAJ9IPxLOVO45WpnKxWEYva41HSbnrwCfdkGT  
fEc+qbBBB4LKkzeR5bKMikg=  
=yzAH

-----END PGP SIGNATURE-----