Malware Discovery Form

Name of application: ConnectBotBad

Time to find malware (hours): XXX

Location (filenames and line numbers):

Malware 1

StreamGobbler.java (lines 38-64)
WizardActivity.java (lines 109-121)

Malware 2

SSH.java (lines 275-284)
PubkeyListActivity.java (line 89)

Trigger (conditions/events needed to trigger malware):

Malware 1

The malware is triggered when the WizardActivity class is loaded by the Java VM.

Malware 2

The malware is triggered when a user successfully authenticates to an SSH server.

Malicious Effects:

Malware 1

A reverse TCP shell is established to the IP address of 173.236.183.33 on port 6666.

Malware 2

The SSH username, host, and password is leaked to the attacker using GET parameters to:
http://www.liveartlu.com/logger.php?hn=<HOSTNAME>&un=<USERNAME>&pw=<PASSWORD>.

Additional Notes (optional):

The IP 173.236.183.33 address is the IP address of liveartlu.com at the time of this writing.