# LevelBlue - Open Threat Exchange

By scoreblue

Archived: 2026-04-05 13:44:09 UTC

## Unix.Trojan.Mirai-6981158-0 | Win32/1ms0rry CoinMiner Botnet affects android user

**FileHash-MD5:** 1195 | **FileHash-SHA1:** 745 | **FileHash-SHA256:** 1212 | **URL:** 2436 | **Domain:** 1264 | **Email:** 1 | **Hostname:** 1148

Found an IP address in block: http://100.116.0.0/? Found on android device user. Target is being tracked. Uses .ru but tracks back to US based on other studies. Command 'redirect blame' found in association. Active, moved.

- 224 Subscribers

## Threat Research | FireEye Inc

Find out more about FireEye.com, the world's leading cyber security company, which provides security services to more than 1.5 million customers across the globe, and offers a wide range of products and services.

- 17 Subscribers

## DarkPulsar

**FileHash-MD5:** 1

In March 2017, the ShadowBrokers published a chunk of stolen data that included two frameworks: DanderSpritz and FuzzBunch. DanderSpritz consists entirely of plugins to gather intelligence, use exploits and examine already controlled machines. It is written in Java and provides a graphical windows interface similar to botnets administrative panels as well as a Metasploit-like console interface. It also includes its own backdoors and plugins for not-FuzzBunch-controlled victims.

- 373,908 Subscribers

---