

GitHub - infoskirmish/hive: The CIA Hive source code as released by Wikileaks

By infoskirmish

Archived: 2026-04-05 13:44:24 UTC

From WikiLeaks:

Today, 9 November 2017, WikiLeaks publishes the source code and development logs to Hive, a major component of the CIA infrastructure to control its malware.

Hive solves a critical problem for the malware operators at the CIA. Even the most sophisticated malware implant on a target computer is useless if there is no way for it to communicate with its operators in a secure manner that does not draw attention. Using Hive even if an implant is discovered on a target computer, attributing it to the CIA is difficult by just looking at the communication of the malware with other servers on the internet. Hive provides a covert communications platform for a whole range of CIA malware to send exfiltrated information to CIA servers and to receive new instructions from operators at the CIA.

Hive can serve multiple operations using multiple implants on target computers. Each operation anonymously registers at least one cover domain (e.g. "perfectly-boring-looking-domain.com") for its own use. The server running the domain website is rented from commercial hosting providers as a VPS (virtual private server) and its software is customized according to CIA specifications. These servers are the public-facing side of the CIA back-end infrastructure and act as a relay for HTTP(S) traffic over a VPN connection to a "hidden" CIA server called 'Blot'. source: <https://wikileaks.org/vault8/>

Source: <https://github.com/infoskirmish/hive>