

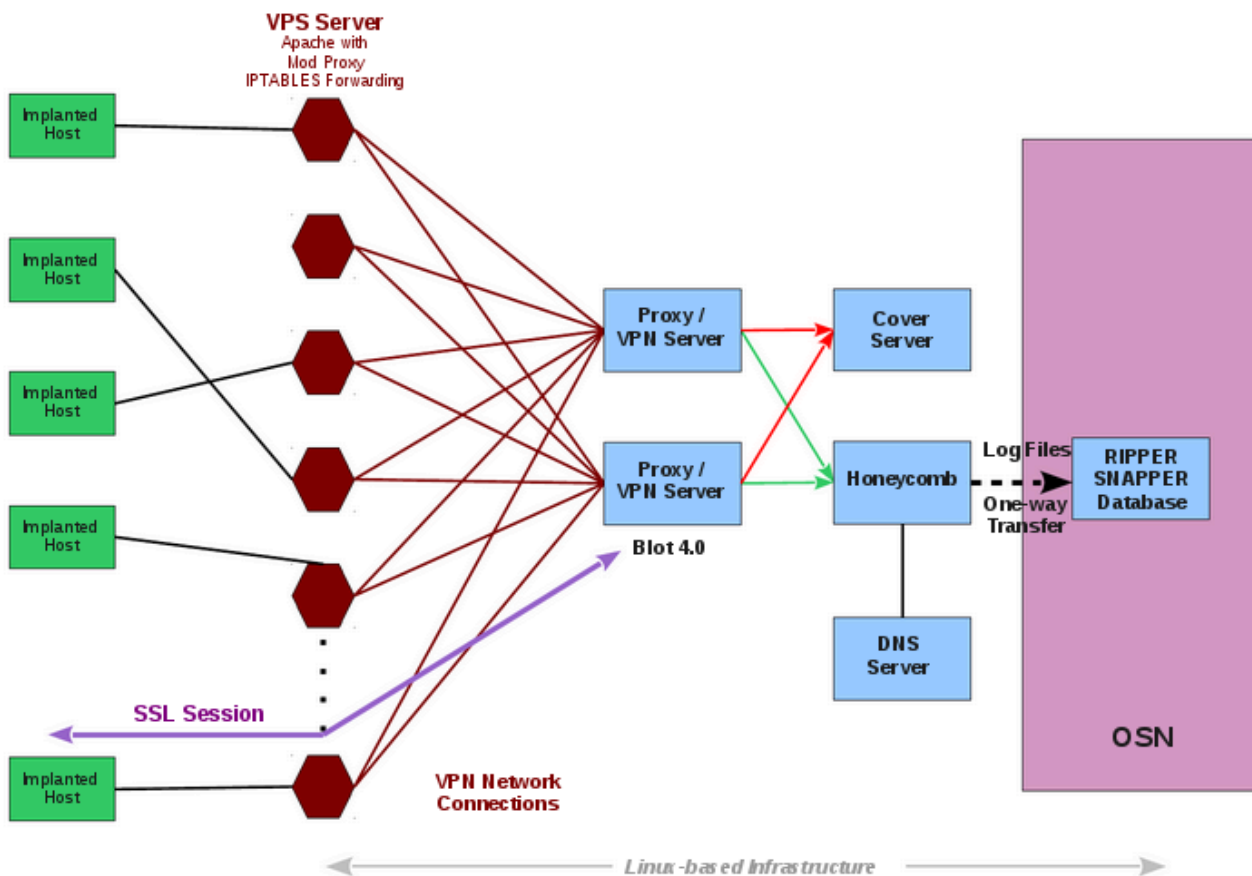
# WikiLeaks - Vault 8

Archived: 2026-04-06 01:15:17 UTC

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'](#).



The cover domain delivers 'innocent' content if somebody browses it by chance. A visitor will not suspect that it is anything else but a normal website. The only peculiarity is not visible to non-technical users - a HTTPS server option that is not widely used: *Optional Client Authentication*. But *Hive* uses the uncommon *Optional Client Authentication* so that the user browsing the website is not required to authenticate - it is optional. But implants talking to *Hive* do authenticate themselves and can therefore be detected by the *Blot* server. Traffic from implants is sent to an implant operator management gateway called *Honeycomb* (see graphic above) while all other traffic go to a cover server that delivers the insuspicious content for all other users.

Digital certificates for the authentication of implants are generated by the CIA impersonating existing entities. The three examples included in the source code build a fake certificate for the anti-virus company [Kaspersky Laboratory, Moscow](#) pretending to be signed by [Thawte Premium Server CA, Cape Town](#). In this way, if the target organization looks at the network traffic coming out of its network, it is likely to misattribute the CIA exfiltration of data to uninvolved entities whose identities have been impersonated.

The documentation for *Hive* is [available](#) from the WikiLeaks [Vault7 series](#).

---

Source: <https://wikileaks.org/vault8/>