Hive

14 April, 2017

Today, April 14th 2017, WikiLeaks publishes six documents from the CIA's HIVE project created by its "Embedded Development Branch" (EDB).

HIVE is a back-end infrastructure malware with a public-facing HTTPS interface which is used by CIA implants to transfer exfiltrated information from target machines to the CIA and to receive commands from its operators to execute specific tasks on the targets. HIVE is used across multiple malware implants and CIA operations. The public HTTPS interface utilizes unsuspicious-looking cover domains to hide its presence.

Anti-Virus companies and forensic experts have noticed that some possible state-actor malware used such kind of back-end infrastructure by analyzing the communication behaviour of these specific implants, but were unable to attribute the back-end (and therefore the implant itself) to operations run by the CIA. In a recent blog post by Symantec, that was able to attribute the "Longhorn" activities to the CIA based on the Vault 7, such back-end infrastructure is described:

For C&C servers, Longhorn typically configures a specific domain and IP address combination per target. The domains appear to be registered by the attackers; however they use privacy services to hide their real identity. The IP addresses are typically owned by legitimate companies offering virtual private server (VPS) or webhosting services. The malware communicates with C&C servers over HTTPS using a custom underlying cryptographic protocol to protect communications from identification.

The documents from this publication might further enable anti-malware researchers and forensic experts to analyse this kind of communication between malware implants and back-end servers used in previous illegal activities.