

## Cofre 8

Código-fonte e análise para projetos de software da CIA, incluindo aqueles descritos na [série Vault7](#) .

Esta publicação permitirá que jornalistas investigativos, especialistas forenses e o público em geral identifiquem e entendam melhor os componentes da infraestrutura secreta da CIA.

O código-fonte publicado nesta série contém software projetado para rodar em servidores controlados pela CIA. Assim como a série anterior do WikiLeaks, Vault7, o material publicado pelo WikiLeaks não **contém** vulnerabilidades de segurança de "dia zero" ou similares que possam ser reutilizadas por outros.



Lançamentos ▼ ▼ ▼

Documentos ▼ ▼ ▼

## Todos os lançamentos

[Hive](#) - 9 de novembro de 2017

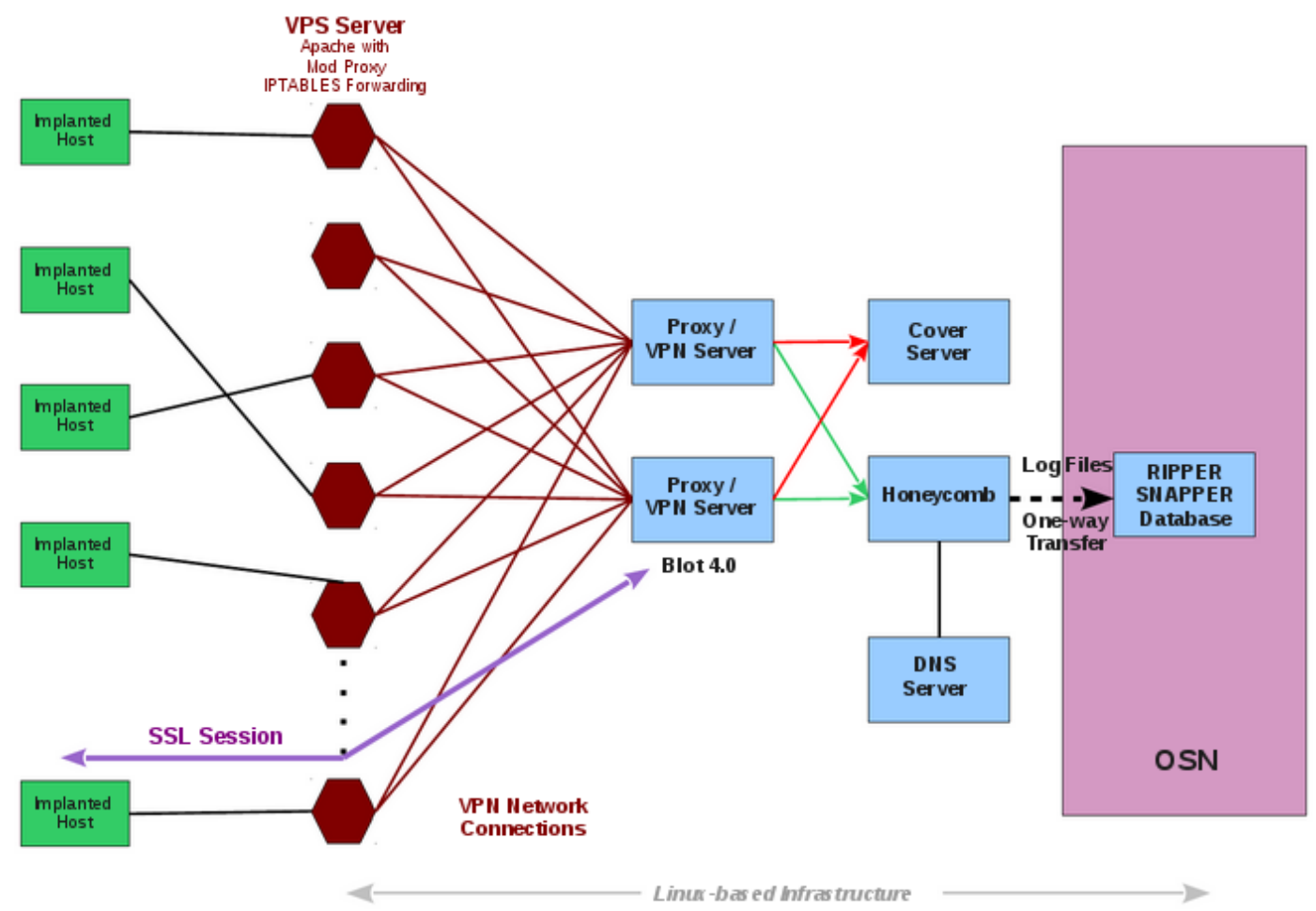
## Colmeia

9 de novembro de 2017

Hoje, 9 de novembro de 2017, o WikiLeaks publica o código-fonte e os logs de desenvolvimento do *Hive* , um componente importante da infraestrutura da CIA para controlar seu malware.

O *Hive* resolve um problema crítico para os operadores de malware da CIA. Mesmo o mais sofisticado malware implantado em um computador alvo é inútil se não houver uma maneira de se comunicar com seus operadores de forma segura e sem chamar a atenção. Usando o *Hive* , mesmo que um implante seja descoberto em um computador alvo, atribuí-lo à CIA é difícil apenas observando a comunicação do malware com outros servidores na internet. O *Hive* fornece uma plataforma de comunicação secreta para uma ampla gama de malwares da CIA, que enviam informações extraídas para servidores da CIA e recebem novas instruções de seus operadores.

O *Hive* pode executar múltiplas operações usando múltiplos implantes em computadores alvo. Cada operação registra anonimamente pelo menos um domínio de cobertura (por exemplo, "dominio-de-aparência-perfeitamente-chato.com") para seu próprio uso. O servidor que executa o site do domínio é alugado de provedores de hospedagem comerciais como um VPS (servidor virtual privado) e seu software é personalizado de acordo com as especificações da CIA. Esses servidores são o lado público da infraestrutura de back-end da CIA e atuam como um retransmissor para o tráfego HTTP(S) através de uma conexão VPN para um servidor CIA "oculto" chamado "**Blot**" .





O domínio de cobertura fornece conteúdo "inocente" se alguém o navegar por acaso. Um visitante não suspeitará que se trata de algo além de um site normal. A única peculiaridade não é visível para usuários não técnicos - uma opção de servidor HTTPS que não é amplamente utilizada: *Autenticação de Cliente Opcional* . Mas o *Hive* usa a *Autenticação de Cliente Opcional* incomum para que o usuário que navega no site não precise se autenticar - é opcional. Mas os implantes que se comunicam com o *Hive* se autenticam e, portanto, podem ser detectados pelo servidor *Blot* . O tráfego dos implantes é enviado para um gateway de gerenciamento do operador de implantes chamado *Honeycomb* (veja o gráfico acima), enquanto todo o outro tráfego vai para um servidor de cobertura que fornece o conteúdo insuspeito para todos os outros usuários.

Certificados digitais para autenticação de implantes são gerados pela CIA, que se faz passar por entidades existentes. Os três exemplos incluídos no código-fonte criam um certificado falso para a empresa de antivírus [Kaspersky Laboratory, em Moscou](#), fingindo ser assinado pela [Thawte Premium Server CA, na Cidade do Cabo](#) . Dessa forma, se a organização-alvo observar o tráfego de rede proveniente de sua rede, é provável que atribua erroneamente a exfiltração de dados pela CIA a entidades não envolvidas, cujas identidades foram falsificadas.

A documentação do *Hive* está [disponível](#) na [série Vault7](#) do WikiLeaks .

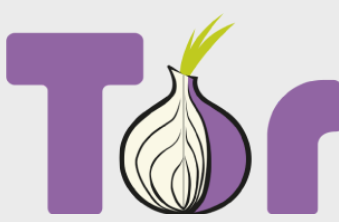
### Documentos vazados

-  Repositório Hive
-  Histórico de Commits do Hive

Principal



Comunidade de Pesquisa WL - pesquisas contribuídas por usuários com base em documentos publicados pelo WikiLeaks.



Tor é uma rede criptografada e anônima que torna mais difícil interceptar comunicações na internet ou ver de onde as comunicações estão vindo ou indo.



Tails é um sistema operacional dinâmico que você pode executar em praticamente qualquer computador a partir de um DVD, pendrive ou cartão SD. Seu objetivo é preservar sua privacidade e anonimato.



A Courage Foundation é uma organização internacional que apoia aqueles que arriscam a vida ou a liberdade para fazer contribuições significativas ao registro histórico.



O Bitcoin usa tecnologia ponto a ponto para operar sem autoridade central ou bancos; o gerenciamento de transações e a emissão de bitcoins são realizados coletivamente pela rede.

