Выпуск реализации анонимной сети I2P 2.2.0

[https://opennet.ru/58792-i2p]

Состоялся (https://geti2p.net/en/blog/post/2023/03/13/new_release_2.2.0) релиз анонимной сети I2P 2.2.0 (https://geti2p.net/en/) и C++-клиента i2pd 2.47.0 (https://github.com/PurpleI2P/i2pd/releases/tag/2.47.0). I2P представляет собой многослойную анонимную распределенную сеть, работающую поверх обычного интернета, активно использующую сквозное (end-to-end) шифрование, гарантирующую анонимность и изолированность. Сеть строится в режиме P2P и образуется благодаря ресурсам (пропускной способности), предоставляемым пользователями сети, что позволяет обойтись без применения централизованно управляемых серверов (коммуникации внутри сети основаны на применении шифрованных однонаправленных туннелей между участником и peer-ами).

В сети I2P можно анонимно создавать web-сайты и блоги, отправлять мгновенные сообщения и электронную почту, обмениваться файлами и организовывать P2P-сети. Для построения и использования анонимных сетей для клиент-серверных (сайты, чаты) и P2P (обмен файлами, криптовалюты) приложений, применяются I2P-клиенты. Базовый I2P-клиент написан на языке Java и может работать на широком спектре платформ, таких как Windows, Linux, macOS, Solaris и т.п. I2pd представляет собой независимую реализацию клиента I2P на языке C++ и распространяется (https://github.com/i2p/i2p.i2p) под модифицированной лицензией BSD.

В новом выпуске реализованы изменения в компонентах NetDB, Floodfill и Peer-Selection, направленные на сохранение работоспособности маршрутизатора в условиях проведения DDoS-атак. В подсистему Streaming добавлена защита от атак, манипулирующих повторной отправкой ранее перехваченных зашифрованных пакетов. В i2psnark добавлены новые возможности для поиска. В транспорты добавлена поддержка ограничения входящих соединений. Повышена эффективность работы списков блокировки.

#I2P

https://docs.google.com/document/d/1KIOFrWYjDAnll3dNTLvcOrAub_pFcyJphoVs4Z_Qv-s/edit?usp=sharing