LNBot: A Covert Hybrid Botnet on Bitcoin Lightning Network

Using Lightning Network (LN) as a botnet command and control infrastructure (C&C) proved to be very resilient against take downs by law enforcements. Unlike previous methods, covert C&C communication over LN provides its botmaster very high anonymity.

Problem Statement and Goals

While various covert Botnets were proposed in the past, they still lack complete anonymization for their servers-botmasters or suffer from slower communications among the botmaster and bots. In this work, we propose LNBot, a new generation hybrid botnet that covertly communicates over Bitcoin Lightning Network (LN) which was recently introduced for faster Bitcoin transactions without writing on the blockchain.

Approach

LNBot is a hybrid botnet having more than 1 C&C server. Commands are sent as series of payments.

Results

We created 100 C&C servers on Bitcoin Testnet. We wrote 2 python scripts that ran on botmaster and C&C servers. Lnd (Lightning Network Daemon from Lightning Labs)’s API.

The cost of running 100 C&C servers is 0.06 bitcoin, which is worth $440 at today’s bitcoin price of $7,360. This is a one time non-recurring investment cost of forming LNBot with 100 C&C servers which is a very small amount considering the fact that each C&C server can control tens of thousands of bots.

Ahmet Kurt
Florida International University