# CISA and FBI Warn Fast Flux is Powering Resilient Malware, C2, and Phishing Networks

Fast flux is a technique used by threat actors to obscure a command-and-control (C2) channel. The approach essentially entails using a variety of IP addresses and rotating them in rapid succession, while pointing to one malicious domain. It was first detected in the wild in 2007 as part of the Honeynet Project. The agencies said threat actors are using the technique to obfuscate the locations of malicious servers, as well as establish resilient C2 infrastructure that can withstand takedown efforts. To secure against fast flux, organizations are recommended to block IP addresses, sinkhole malicious domains, filter out traffic to and from domains with poor reputations, and enforce phishing awareness and training.