# TTP Detail – T1584.005

## TTP Information

Name: Botnet

Description: Adversaries may compromise numerous third-party systems to form a botnet that can be used during targeting. A botnet is a network of compromised systems that can be instructed to perform coordinated tasks.(Citation: Norton Botnet) Instead of purchasing/renting a botnet from a booter/stresser service, adversaries may build their own botnet by compromising numerous third-party systems.(Citation: Imperva DDoS for Hire) Adversaries may also conduct a takeover of an existing botnet, such as redirecting bots to adversary-controlled C2 servers.(Citation: Dell Dridex Oct 2015) With a botnet at their disposal, adversaries may perform follow-on activity such as large-scale [Phishing](https://attack.mitre.org/techniques/T1566) or Distributed Denial of Service (DDoS).

## Threat-Mapped Scoring

Score: 1.5

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: resource-development

## APTs (Intrusion Sets)

* Axiom
* HAFNIUM
* Sandworm Team
* Volt Typhoon