# TTP Detail – T1583.005

## TTP Information

Name: Botnet

Description: Adversaries may buy, lease, or rent a network of compromised systems 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) Adversaries may purchase a subscription to use an existing botnet from a booter/stresser service.

Internet-facing edge devices and related network appliances that are end-of-life (EOL) and unsupported by their manufacturers are commonly acquired for botnet activities. Adversaries may lease operational relay box (ORB) networks – consisting of virtual private servers (VPS), small office/home office (SOHO) routers, or Internet of Things (IoT) devices – to serve as a botnet.(Citation: ORB Mandiant)

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).(Citation: Imperva DDoS for Hire)(Citation: Krebs-Anna)(Citation: Krebs-Bazaar)(Citation: Krebs-Booter) Acquired botnets may also be used to support Command and Control activity, such as [Hide Infrastructure](https://attack.mitre.org/techniques/T1665) through an established [Proxy](https://attack.mitre.org/techniques/T1090) network.

## Threat-Mapped Scoring

Score: 1.5

Priority: P4 - Informational (Low)

## Kill Chain Phases

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

## APTs (Intrusion Sets)

* APT5
* HAFNIUM
* Ke3chang