Acquire Infrastructure: Botnet, Sub-technique T1583.005 - Enterprise

Archived: 2026-04-05 17:39:36 UTC

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.[1] 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.[2]

With a botnet at their disposal, adversaries may perform follow-on activity such as large-scale Phishing or Distributed Denial of Service (DDoS).[3][4][5][6] Acquired botnets may also be used to support Command and Control activity, such as Hide Infrastructure through an established Proxy network.

Source: https://attack.mitre.org/techniques/T1583/005