Botnet Anatomy

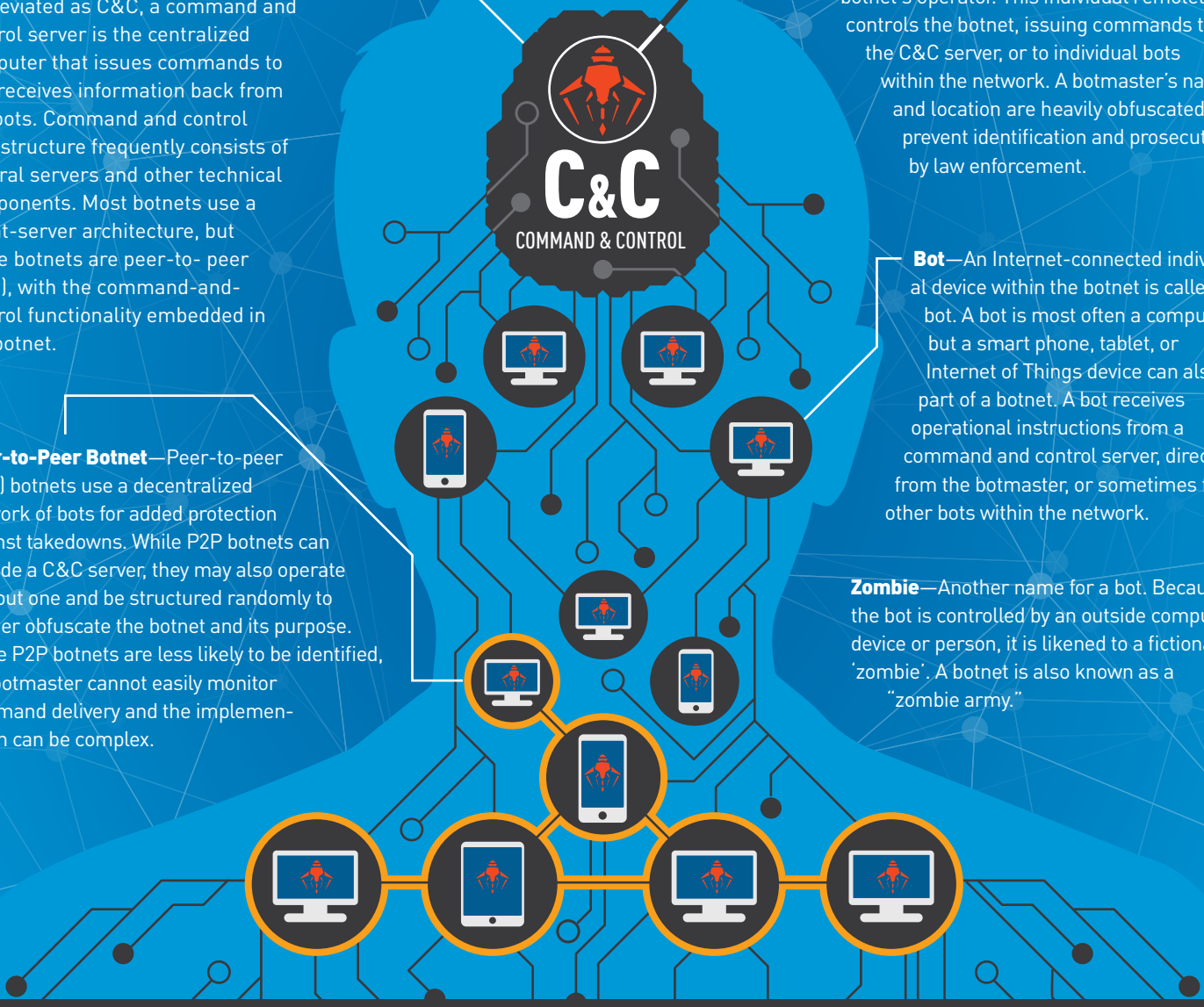
CYREN

Botnet—A botnet is a network of Internet-connected and malware-infected devices, which have been co-opted by cybercriminals. It is used to distribute spam and malware, or launch distributed denial-of-service attacks. Botnets can grow to 1,000,000 devices, and have been known to send up to 60 billion spam emails in a day. The term 'botnet' derives from the combination of the words "roBOT NETwork."

CYBERCRIMINAL (BOTMASTER)

Botmaster—Alternatively called a botnet controller or bot herder, the botmaster is the botnet's operator. This individual remotely controls the botnet, issuing commands to the C&C server, or to individual bots within the network. A botmaster's name and location are heavily obfuscated to prevent identification and prosecution by law enforcement.

Command and Control Server—Often abbreviated as C&C, a command and control server is the centralized computer that issues commands to and receives information back from the bots. Command and control infrastructure frequently consists of several servers and other technical components. Most botnets use a client-server architecture, but some botnets are peer-to- peer (P2P), with the command-and-control functionality embedded in the botnet.



Bot—An Internet-connected individual device within the botnet is called a bot. A bot is most often a computer, but a smart phone, tablet, or Internet of Things device can also be part of a botnet. A bot receives operational instructions from a command and control server, directly from the botmaster, or sometimes from other bots within the network.

Peer-to-Peer Botnet—Peer-to-peer (P2P) botnets use a decentralized network of bots for added protection against takedowns. While P2P botnets can include a C&C server, they may also operate without one and be structured randomly to further obfuscate the botnet and its purpose. While P2P botnets are less likely to be identified, the botmaster cannot easily monitor command delivery and the implementation can be complex.

Zombie—Another name for a bot. Because the bot is controlled by an outside computing device or person, it is likened to a fictional 'zombie'. A botnet is also known as a "zombie army."

How a C&C Botnet Distributes Malware

1
A botmaster develops a botnet by distributing bot malware to infect PCs or other devices. He may also rent an existing botnet from another criminal.

2
The newly harvested bots or "zombies" report in to the botnet's command and control (C&C).

3
The C&C now controls these bots and issues instructions for the bot to distribute executable malware files, as well as the email templates and potential victim address lists.

4
The infected zombie bots receive the orders, each sending email messages carrying the malware payload to thousands of potential victims.