Find out if you are vulnerable to botnet: https://www.ixiacom.com/products/breakingpoint
Block connections to botnet controllers: https://www.ixiacom.com/products/threatarmor

Is Your Company's Network Part of a Botnet?

Do you already have an infected machine in your network?

The botmaster sends out malware to take control of other computers. The computer is now a zombie and can be controlled from the botmaster's command server.

1. If the malware is executed, the computer is compromised and joins the botnet.

How a Botnet is Formed

Methods of Infection
- Spam email
- Malicious websites
- Files distributed by social media

Causes of Infection
- No protection on device
- Infrequent updates
- Lack of user education

83% of organizations had existing bot infections in 2014
2.2X more data breaches by companies slow to react to botnet threats

Zeus
Graftor
Ramnit
Conflicker
Sality
Smokeloader
Ramdo
Gamarue

51,848,194
Steals banking credentials
21,673,764
Downloads malicious files
12,978,788
Steals banking credentials
12,357,794
Disables system security, attacker gains remote access
11,791,594
Steals sensitive information
9,417,333
Installs malware
5,771,478
Performs click-fraud
3,329,930
Opens a backdoor for attacks

Hackers Use Zombie Computers For
- DDos Attacks
- Sending Spam
- Click Fraud
- Data Theft
- Identity Theft
- Attacks for Hire

Botnet Example: CryptoWall Spread by Click Fraud Botnet

Botnet operators use zombie computers to run click fraud. Botnet operators recognize flash vulnerability. Install CryptoWall on zombie computers. Encrypt user data and demand ransom.

Cryptowall is a type of "ransomware," malware that installs itself on a computer, encrypts files rendering them useless to users, and demands a ransom payment to decrypt the data.

In June 2015, a botnet known as "RuthlessTreeMafia" changed its focus. The botnet was originally used for click fraud—it would open hidden browser windows on users' computers and use them to generate fake clicks on advertising banners.

The botnet's operators leveraged their hold on large numbers of user machines and, instead of just click fraud, started installing CryptoWall on those machines. They were probably exploiting a "zero day vulnerability" in Adobe Flash, which allowed an attacker to install files on a user's computer.

The end result was large numbers of machines infected by dangerous ransomware and damages estimated in millions of dollars.