Is Your Company's Network Part of a Botnet?

How a Botnet is Formed

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

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

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.

Comparison of botnet infections

Spike due to zero day exploit

Source: Cisco Security Research

Botnet Infections in Company Networks

Cisco analyzed the networks of 121 companies from April to October 2015 for evidence of one or more of eight commonly seen botnets.

This graph represents the number of users on these networks infected with different botnet malware.