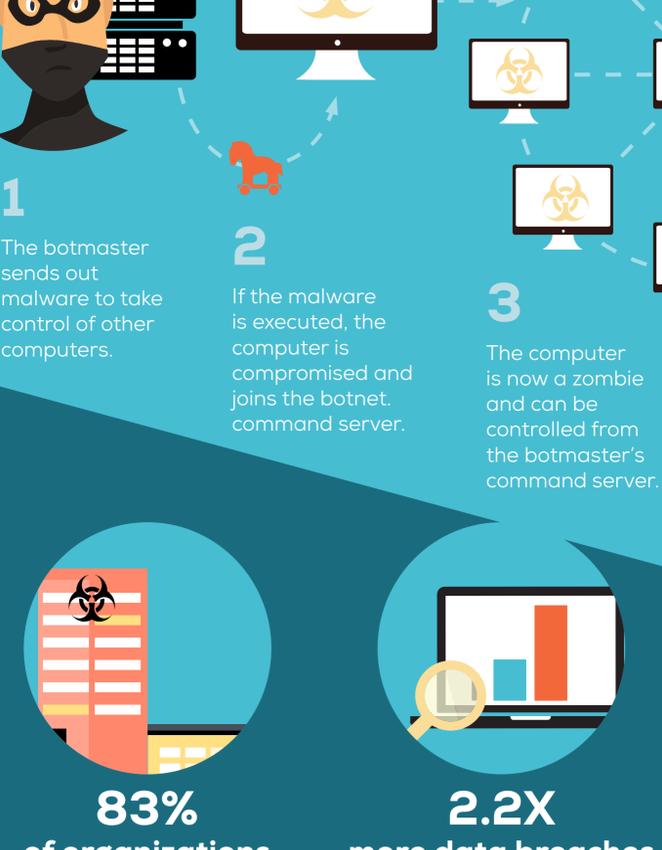


Is Your Company's Network Part of a Botnet?

How a Botnet is Formed



Methods of Infection



Causes of Infection



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

Hackers Use Zombie Computers For



Botnet Example: CryptoWall Spread by Click Fraud Botnet

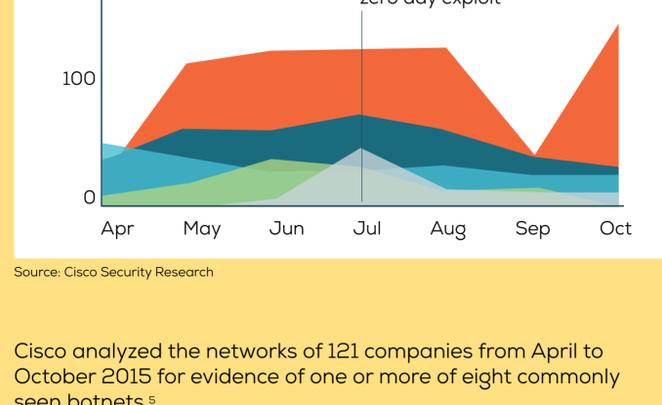


Cryptowall is a type of "ransomware," malware that installs itself on a computer, encrypts files rendering them useless to users, and demands a ransom payment to decrypt the data.

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.³ They were probably exploiting a "zero day vulnerability" in Adobe Flash, which allowed an attacker to install files on a user's computer.⁴

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

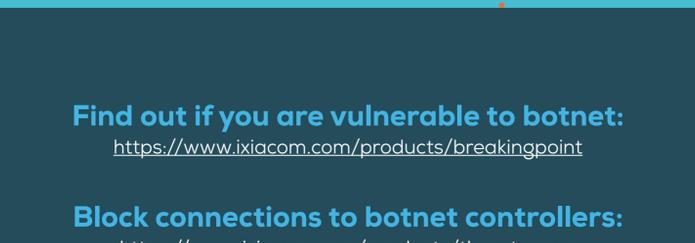
Botnet Infections in Company Networks



Cisco analyzed the networks of 121 companies from April to October 2015 for evidence of one or more of eight commonly seen botnets.⁵

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

Do you already have an infected machine in your network?



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>

ixia
A Keysight Business

WE MAKE NETWORKS STRONGER