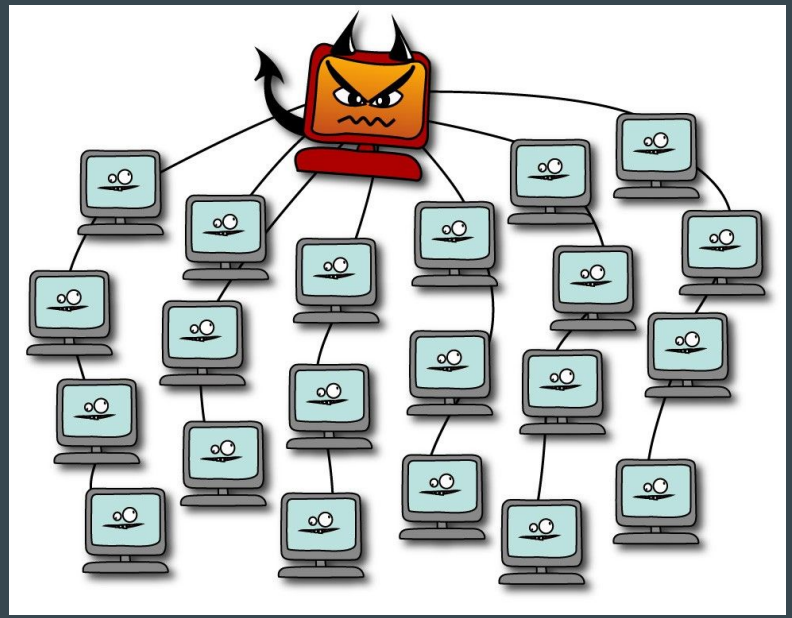
Botnets

A Crash Course

Sason Baghdadi

What is a botnet?

- A network of infected machines controlled by one or many hackers
  - Client-Server and Peer-to-Peer network models
    - We'll be focusing on the Client-Server model
  - Botnet sizes have been reported as low as a few hundred machines up to over a million machines
- The network of machines work together to accomplish the botnet master's goal(s)

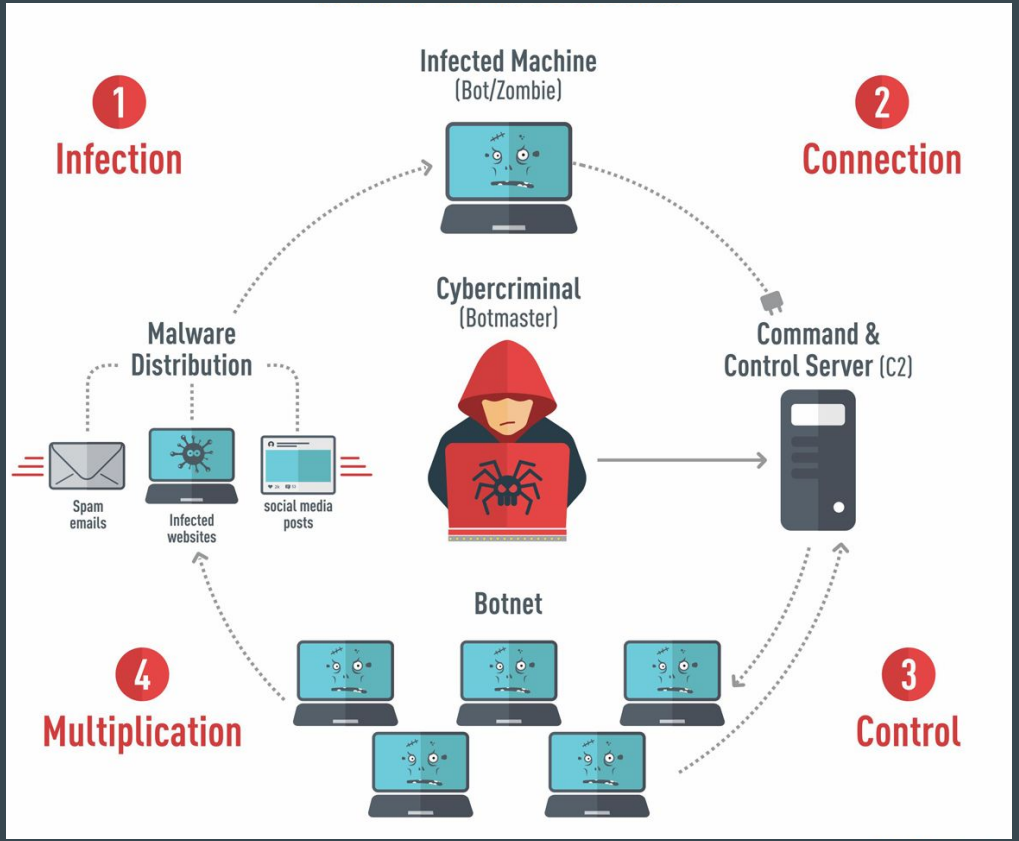


What are botnets capable of?

- Emailing spam out to millions of Internet users
  - Using the spam to spread malware which, in turn, causes newly infected machines to email spam and spread malware
- Using your machine's power to assist in distributed denial-of-service (DDoS) attacks to shut down servers
  - E.g. Mirai botnet against Dyn DNS Server (2016)
    - Disrupted an entire day of service for: Amazon, CNN, GitHub, Netflix, Twitter, Visa, etc.
- Financial gains for the botnet master
  - Ransomware
  - **Provide other hackers access to your computer**
  - Bank fraud
  - Intellectual property theft, e.g. government and business secrets

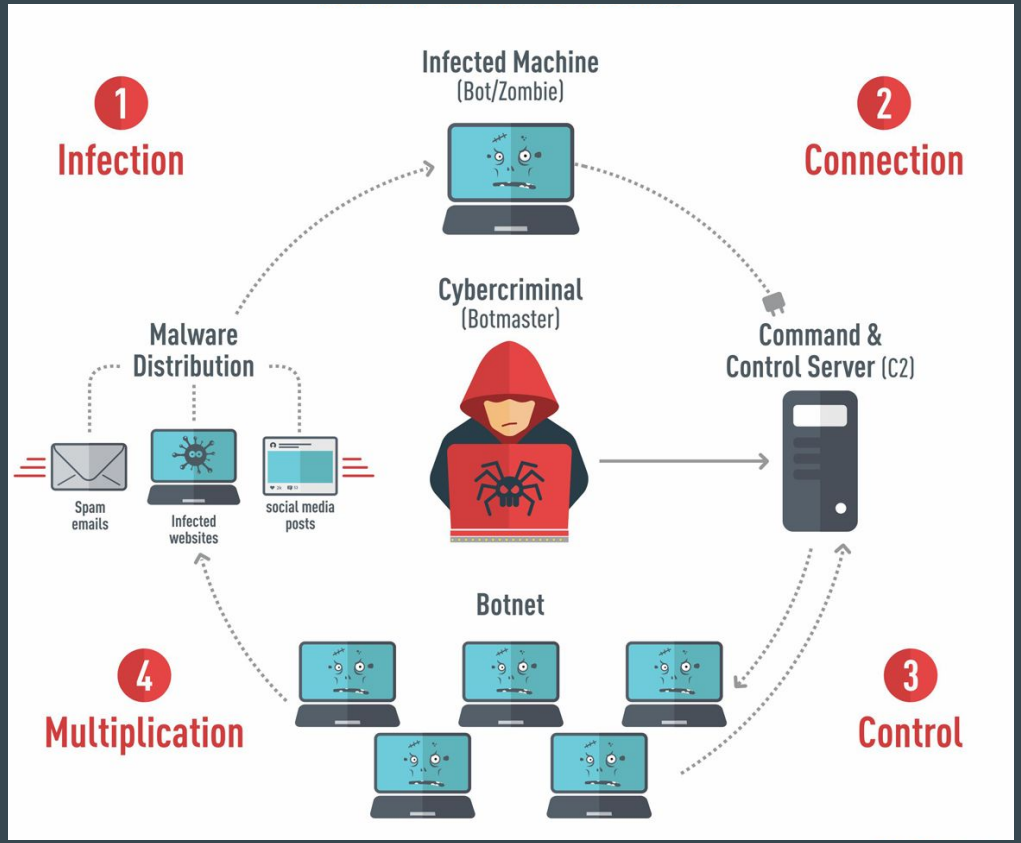
How do botnets work? - 1. Infection

1. Cyber criminal (botnet master) spams emails packed with malware to millions of users
2. User opens a suspicious email in their spam folder
3. User downloads attachment or clicks link and is infected with malware upon opening
    a. prince_of_nigeria.pdf/.zip/.word
    b. FREE_VIAGRA.com/.ru



How do botnets work? - 2. Connection

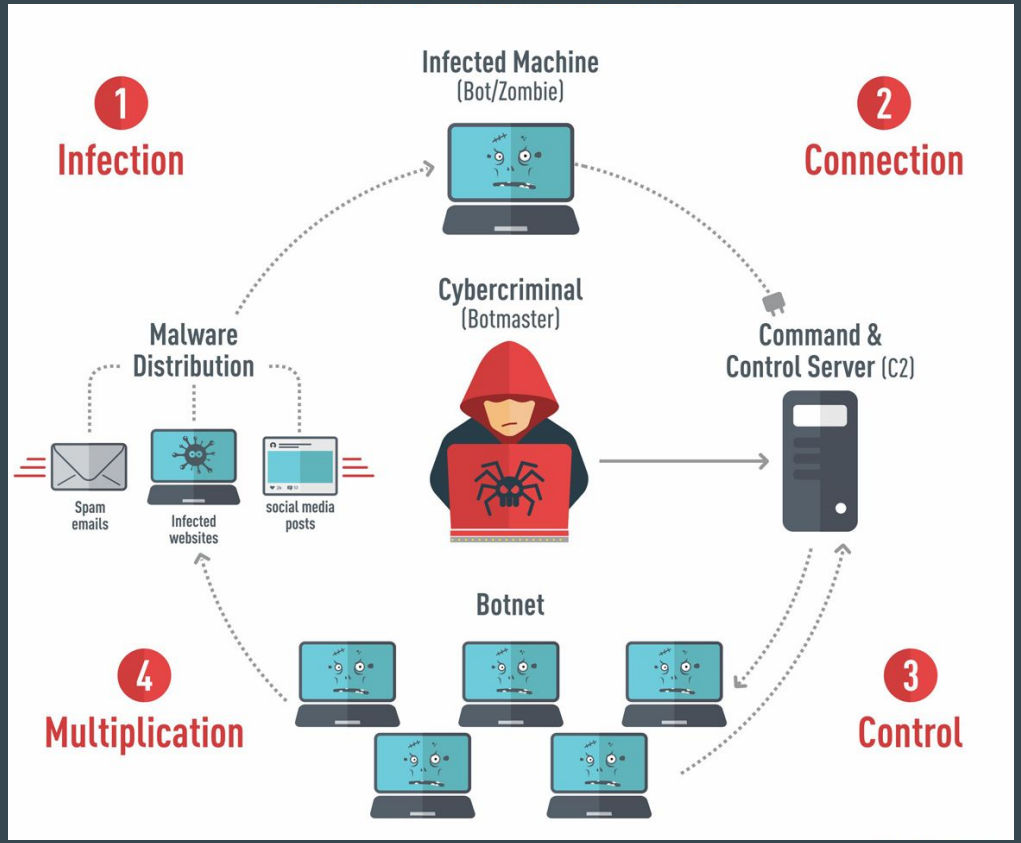
1. The malware automatically sends a request to join the botnet
   a. Request is sent through email, IRC, Pastebin, etc.
   b. Typically heavily encrypted or hidden inside regular traffic
2. Botnet requests for authentication
   a. Usually through some hard-coded key, api call, etc.
3. User's unknowingly joins the botnet and allows the botnet master access to the computer



How do botnets work? - 3. Control

The botnet master can now:

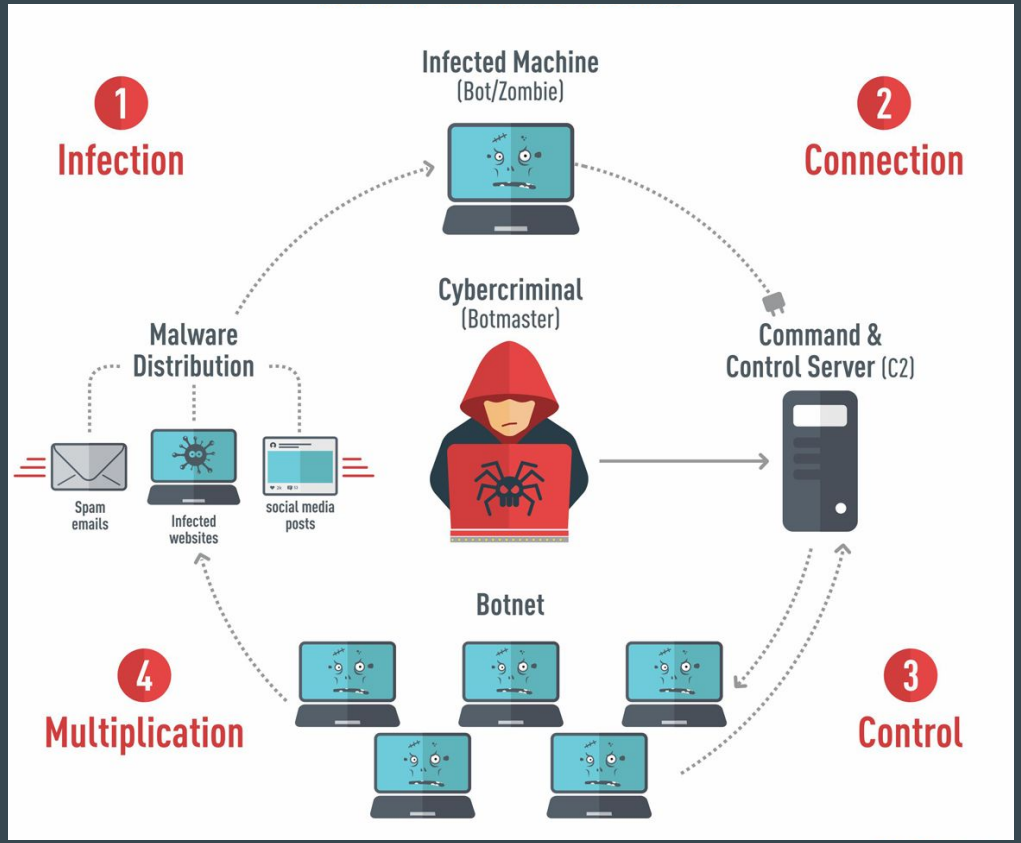
1. Issue remote commands to the user's machine
   a. Spam email to infect more machines
   b. DDoS attack
   c. Financial gain
2. Upload data to user's machine
   a. Keylogger to steal banking credentials
   b. Update malware's functionality
3. Download from user's machine
   a. System information
   b. Banking credentials
   c. Intellectual property



How do botnets work? - 4. Multiplication

Malware begins propagating as programmed:

- Spam email to others with malicious links, attachments, etc.
- Search through the machine's local network for vulnerable machines
  - Perform DNS poisoning attacks to users on the same network
- Search through the public network for vulnerable machines
- Do nothing



Example - Python-Based Crypto-Miner Botnet (01/2018)

Analysis:
https://www.f5.com/labs/articles/threat-intelligence/new-python-based-crypto-miner-botnet-flying-under-the-radar?sf178360556

- Python malware exploiting jboss serialization vulnerability
- Infected 1,000+ Linux systems to mine cryptocurrency
  - Host/DNS/OS name
  - Number of CPUs, RAM, etc.
  - CPU usage
- Used **public** pastebin posts as a C&C resource center for the slaves
- Mined over $60,000 at the time of discovery
- No idea of overall profit made overall as it's an ongoing case

Example - Gameover ZeuS Botnet

Story: https://www.wired.com/2017/03/russian-hacker-spy-botnet/

- The initial version, ZeuS, was a swiss-army-knife trojan
  - Ransomware, banking theft, man-in-the-middle attacks, keyloggers, etc.
  - Infected estimated 3.5 million PC since 2007, “retired” by botnet master in 2010
    - Zeus code went public in 2011
  - Over 100+ arrested in Ukraine, USA, UK, ~$70 million stolen
  - Analysis: https://talosintelligence.com/zeus_trojan

- Gameover ZeuS reborn as encrypted peer-to-peer network
  - Instantly connects to C&C server, disables certain system processes, deletes essential system files
  - Used largely for banking fraud and distribution of CryptoLocker ransomware
  - Taken down in late 2014 with the help of FBI, 10 partner countries, countless security agencies
    - Multiple failed attempts, malware updated to become more secure after each failed attempt
  - Over 1 million infections globally, 25% in USA
  - Global losses estimated in the hundreds of millions of dollars

Detecting botnet/malware infections

- Monitor your network traffic for suspicious websites/IP addresses
  - Free tools such as:
    - Wireshark
    - Tcpdump
    - Router's built-in IDS
  - Cross-check suspicious IP addresses with SonicWall's botnet IP lookup
    - http://botnet.global.sonicwall.com/view
- Keep an eye out for suspicious processes
  - Why is iexplorer.exe running when I only use Firefox?
  - Why is there a python process running?
- PC slowing down, high CPU usage, weird interactions/glitches

Preventing botnet/malware infections

- Update your operating system, software, firmware, etc.
- Don’t click on links you don’t trust
- Don’t fall for spam emails
- Close all unused ports from the internet
  - If you need some ports open, make sure the services running on the ports are secure
- Change default passwords of anything and everything in sight
- Download an antivirus software and actually use it
  - E.g. Malwarebytes Anti-Malware, AVG, etc.
- **Use common sense**

Keeping up with botnet/malware news

Cisco Talos Group: https://blog.talosintelligence.com/

MalwareTech: https://www.malwaretech.com/

Krebs on Security: https://krebsonsecurity.com/

Kaspersky Lab's Securelist: https://securelist.com/

F5 Labs: https://www.f5.com/labs

The Hacker News: https://thehackernews.com/

Twitter: Cyber security enthusiasts primarily spread news through Twitter