Summary
- Shift in primary motivation for hacking in the hacker community
- Botnets pose the biggest threat to the Internet community.
  - Thousands of computers controlled by a single (or a small group of) hacker can coordinate attacks.
  - Damage caused is much greater.
  - Botnets are getting more sophisticated
- Paper aims at better understanding of botnet behavior by presenting a simple taxonomy of botnets.

Background
- Botnets – Pools of compromised computers that are under the controls of a single hacker, (or a group of hackers) known as \textit{botmaster}.
- Bot – a compromised end host or a computer which is member of a botnet.
  - Also a malicious executable that compromises, controls and recruits computer hosts into a botnet.

Taxonomy
- Attacking Behavior
- Command & Control (C&C) models
- Rallying Mechanisms
- Communication protocols
- Observable botnet activities
- Evasion techniques
**Attacking Behavior**

- The method used for attacking to achieve their ultimate goals.
- Four aspects:
  - Infecting new hosts
  - Stealing personal information
  - Phishing and spam proxy
  - DDoS

**Attacking Behavior: Infecting new hosts**

- Malicious email with a catchy subject and infected attachment (resembling jpeg)
- User will be duped into clicking it → Execute.
- Host compromised.
- OR Scan a subnet & Actively search for common Windows vulnerabilities (DCOM, LSASS)
- Launch attack to compromise host
- Spread (Botnet can be exposed because a bot would generate a burst of small packets when actively searching for other vulnerable targets)

**Attacking Behavior: Stealing Sensitive Information**

- Use keyloggers and network traffic sniffs to steal sensitive information from the infected-host.
- Sensitive data is compiled in digest format and sent to botmaster (using IRC channel created by botnet or emails)

**Attacking Behavior: Sending Spam**

- Botnets used to disseminate spams.
- Advantages
  - Victims can’t trace spam back to source
  - Availability of aggregate computing power and bandwidth to distribute large amounts of spam
- Attacks:
  - Spam tricks hosts to visit malicious websites to install malware by exploiting OS vulnerabilities.
  - Advertise illegal merchandise
  - Launch phishing attacks to steal identity

**Attacking Behavior: DDoS**

- Botnets used to launch DDoS attacks against large organizations.
- Also used for extortions
- Use UDP Flooding, TCP SYN flooding and HTTP Flooding
Command and Control (C&C)

- Typically an IRC Server.
- C&C are unique, unlikely to change amongst bots.
- C&C is essential to support an effective & operational botnet.
- The weakest link.

C&C Server: Centralized

- Botmaster sets up a C&C server (it maybe a bot itself).
- Bots connect to C&C server after infection (by joining a certain IRC Channel & listen to messages) and wait for botmaster’s commands. Commands include:
  - Scan the subnet for vulnerable hosts
  - Adversaries use 205.4.25.1 and more.
  - Download a malware from a LUR
  - c:/my32awd.exe 1
  - Run a syn flood attack
  - adash.com 133.98.8.120 21 200
- In reality, C&C servers use various architecture to issue commands.

C&C Server: P2P

- Use ideas of P2P communication to control botnets
- Strengths:
  - Resilient to network failures
  - Hard to discover and destroy. Destroying one or even multiple bots won’t cause destruction of the botnet.
- Weaknesses:
  - Existing P2P systems support conversations of a small group of users (usually 10-50)
  - No guarantees of message delivery and propagation latency. Harder to control and coordinate attacks than centralized C&C.

C&C

- Centralized Model
- Peer-to-peer (P2P) Model
- Random Model
C&C Server: Random

- Aims at high survivability
- A bot doesn’t contact other bots or botmaster actively.
- Bot listens to incoming connections to its botmaster.
- Botmaster has to scan the internet to discover bots and then issue commands
- Not yet used in real world.
- Strengths:
  - Easy to implement
  - Resistant to discovery and destruction
- Weaknesses
  - Difficult to coordinate for large scale attacks

Rallying Mechanisms

- How bots are coordinated by their botmasters.
- Classifications:
  - Hard-coded IP address
  - Dynamic DNS Domain name
  - Distributed DNS Service

Rallying Mechanisms: Hard coded IP address

- IP address of C&C server is hard coded into the binary at the bot.
- Problem: C&C server can be easily detected and communication channel can be easily blocked
- Not much used by current bots.

Rallying Mechanisms: Dynamic DNS Domain name

- Hard coded domain names, assigned by dynamic DNS providers, are hard coded into the binary at the bot.
- Strengths:
  - Even if the C&C server is shut down, the botmaster can create a new server elsewhere and update the IP address in the DNS entry
  - Harder to catch botmaster. Activities can be resumed quickly and bots can be directed to new C&C server.

Rallying Mechanisms: Distributed DNS Server

- Botnets run their own DNS Service (at locations outside reach of law)
- Binary at bots includes address of these DNS servers and contact them for IP resolution.
- Usually, these DNS services are run at high port numbers to evade detection by security devices.
- Hardest to detect and destroy.

Communication Protocols

- Botnets use well defined communication protocols.
- Studying the communication characteristics provides understanding of their origins and software tools used.
- Helps security researchers to decode their conversations for detection and destruction of the botnets
- Classifications:
  - IRC
  - HTTP
  - Other Protocols
Communication Protocols: IRC

- Most common protocol used for botnets.
- Mainly designed for group communication in discussion forms called “channels”.
- Allow one-to-one interactions using private messages.
- Botnet C&C server runs a standard IRC service, creates a designated channel.
- IRC bots have scripts that parse messages sent in their channel.
- Bots connect to service and join the predefined channel and wait for commands which are hidden in messages.
- Easy to coordinate attacks.
- Hard to block IRC traffic tunneled in HTTP.
- Firewalls can be configured to block IRC traffic in corporate environments.
- Network admin can look at the amount of incoming and outgoing IRC traffic.

Communication Protocols: HTTP

- Use HTTP to maintain botnet communication.
- Bots contact C&C using HTTP
  - http://hostnames/reg?u=ABCDEF01&v=114
- C&C server responds with a HTTP request, which may contain commands to execute update or program, scan network etc.
  - upd, exe, inc, scv, prj, spd
- Strengths:
  - HTTP makes bots harder to detect
  - Firewalls block IRC ports but not HTTP.
- Weaknesses:
  - Still can be detected using appropriate filters.
  - Bot HTTP Traffic is different from normal traffic (for example, Response will have abnormal HTTP header fields or abnormal payload)

Communication Protocols: Other protocols

- Advanced botnets use other protocols such as IM, P2P for communication.
- Evidence of some botnets using WASTE (encrypted P2P protocol for private messaging and file transfer between trusted parties).

Evasion techniques

- New botnets are more evasive to AV engines and signature based intrusion detection systems (IDS) and more evasive to anomaly based detection systems.
- Have added mechanisms to hide traces.
  - Use modified IRC protocols or new protocols (HTTP, VoIP) for communication.
  - Encryption schemes to prevent content revelation.
  - Use convert channel communication (TCP, ICMP, IPv6 tunneling)
- Detection and destruction of C&C can be achieved using some techniques such as mechanisms based on anomaly network behavior.

Other observable Activities

- Knowledge of abnormal behavior (global and local) is key to detect presence of botnets.
  - Network based behavior
  - Host based behavior
  - Global correlated behavior

Other observable Activities: Network Based Behavior

- Botnets generate certain observable network traffic patterns that can be used to detect bots and C&Cs.
- Observable Communication:
  - Abnormal IRC & HTTP Traffic patterns. E.g. inbound/outbound IRC traffic to interior enterprise network & not human-understandable IRC syntax conventions.
  - Abnormal DNS queries. Improper DNS names cheese.dns4biz.org
  - Detect that particular domain keeps changing IP address frequently.
  - Bots are usually idle, but generate responses faster than humans.
  - Bussy traffic
**Other observable Activities: Network Based Behavior**

- Observable Attacking behavior
  - Botnets send out large number of TCP SYN packets with invalid IPs (inside subnet) (DDoS attack)
  - Internal host sends out phishing emails $\Rightarrow$ bot

**Other observable Activities: Host Based Behavior**

- Certain observable like viruses
- Bots will make a sequence of system/library calls (modifying system registry, creating network connections, disabling AV programs) different from legitimate programs.
- Other hints
  - AV Programs fail to update

**Other observable Activities: Global correlated Behavior**

- Global behavior of botnets can be used for efficient detection.
- Don’t change for different botnet architectures.
- Example
  - When using Dynamic DNS, if C&C server changes, bots will be disconnected from previous C&C.
  - They will query DNS Server for new IP address $\Rightarrow$ increase in number of DNS queries. Network monitor can detect this.

**Thank You!**