DISCUSSION 6/3/20

BOTNETS

ANNOUNCEMENTS

- PA5 due June 4th @ 12:30 PM PDT
  - Absolute late submission cut off June 11th @ 12:30 PM PDT (grades due)

AGENDA

- Botnet Architectures
- Generic Countermeasures
- Applications
- Open Office Hours

FUNDAMENTAL COMPONENTS

Botnet

A network of compromised systems with a common command and control system (C_2)

Controller

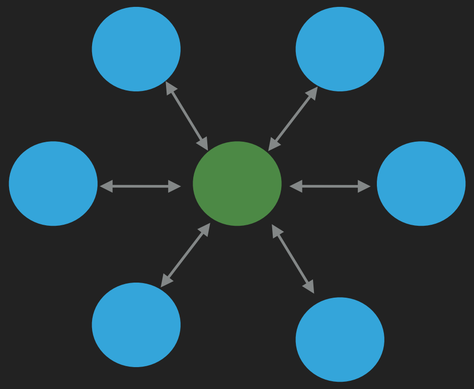
Agent that manages compromised systems via command and control system

The command and control system ties the network together and provides and interface for the controller

COMMAND AND CONTROL STRUCTURES: NETWORK ARCHITECTURE

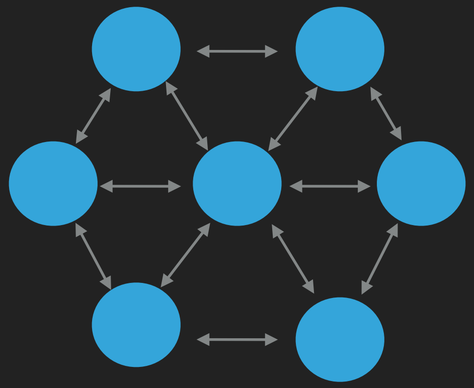
Centralized

- One or several hosts act as control hubs directing activity of botnet
- Provides single point of failure
- Round Robin of several hosts as C_2 helps, but still compromised if the set of hosts is



Peer-to-peer (Decentralized)

- All bots are fungible (any bot can take on any role)



COMMAND AND CONTROL STRUCTURES: COMMAND ISSUANCE

Push

- Controller issues commands to bots

Pull

- Idle bots request work

RESILIENCY/RECOVERY

Auto-update bots

- Add counter-counter measures, alter architecture or behavior, etc.

Command and Control

Round Robin - (think ordered list of hosts to treat as command center)

Domain Generation Algorithm - pre-arranged hash function for determining new command domain

Digital Signatures - commands and updates come with signatures (lost command and control host cannot issue ‘cleanse’ command

DETECTION

Sniff Traffic

- destinations - blacklisted C_2s or ML to detect anomalous behavior

(counter-measure: peer-to-peer architecture)

- content - keywords, command signatures, etc

(counter-measure: encryption)

Self Infection

- Purposefully infect controlled system to study bot induced behavior

(counter-measure: black-list bad bots)

Hijack C_2

- Reroute C_2 through monitor system to map botnet

(difficult to pull-off and legally challenging)

ELIMINATING BOTNETS

- Legal action against controller
- Dismantle botnet
  - shutdown C_2, blacklists, cleaning incentives
  - Issue cleanse command over C_2?
    - Legally infeasible
    - Opt-in approach (Microsoft has customers opt-in up front)

NECESSITY IS THE MOTHER OF INVENTION

- Blacklisting of known spam IP addresses as well as proxies
  - Spammers need method of sending spam via many IPs
  - Build botnets via malware

What works for one will work for many…

- Build and sell botnet (platform)
- Build and sell botnet with SPAM, piracy, phishing, DDos, (application)

CHECK PLEASE

Botnet value determined by:

- Generic Resources: Hardware (cpu, storage, etc.)
- Unique Resources: account credentials, intellectual property, etc.

Most ‘cash out’ along a spectrum of advertising and theft

ADVERTISING BASED MONETIZATION

- Click Fraud
  - Pay to have botnet click competitor's ads
- Spam

  Marketing
  - Selling real or counterfeit goods and services
  - Stock price manipulation

  Attraction (direct recipients somewhere)
  - Phishing, XSS, CSRF, drive-by malware

  Malicious Attachments

COUNTERING SPAM

SMTP characteristics enabling spam

- Mail is unencrypted and unauthenticated
- Mail can be sent from any host regardless of source domain (spoofing)

Counter Measures

- blacklists- mark spam sources based on honeyclients, user reports, ML
- authentication
  - SPF: DNS lookup of domain/IPs authorized to mail under domain
  - DomainKeys: Digital signature in header, DNS lookup of public key for verification
- content filtering: keywords, heuristics such as ALL CAPS or spoofed header
- ML

THEFT END OF THE SPECTRUM

Infostealers

Method: Gather user credentials and return to controller via C_2 or ‘dead drop’

Counter: 2-factor authentication

- Can be side-stepped by allowing user to perform authentication

Monetization:

- Direct:

  “white plastic”- victim’s data burned onto card

  wire transfer- typically to account where “money mule” withdraws (division of risk)

- Indirect:

  Purchase goods and resell

THEFT END OF THE SPECTRUM

Fraud

Fake anti-virus warns system infected but can be cleaned for $$

Extortion

Issue threat to victim (real or not) unless fee is paid

- Claim to be law enforcement offering to drop investigation for $$
- Ransomware - encrypt files offering to unencrypt for $$ or else throw away key