Botnet research, Mitigation and the Law

Alexander Muentz
ShmooCon 2008

Disclaimer

- I am an attorney, just not your attorney
- This talk is for edutainment purposes only
- This field of law is in flux- what is correct today may not be so next year
- Local laws vary
- Contents may settle during shipping
- Special thanks to Jose Nazario and the Shmoocon organizers

Why this talk is relevant

- Laws designed to protect users & systems are broad and vague
  - Lots of discretion in the prosecution's hands
  - 'Myth of the Super-User' is alive and well
- Researchers & IT security are easily reached
  - compared to computer criminals
  - to a jury, 'freelance security researcher' and 'evil computer hacker' may look alike
- FUD alert
  - Lots of this is hypothetical- be wary, not alarmed

Wiretap Act

- 18 USC 2511 (Wiretap Act)
  - Regulates the use of wiretaps, sniffers and full content network monitoring and divulging the contents
  - Broad prohibition against 'interception'
    - Contemporaneous (with transmission)
    - Acquisition (of)
    - The *contents* of an electronic transmission
  - Also criminalizes the *distribution* of illegally obtained communications

Wiretap Act, Continued

- Exceptions to prohibition on capture
    - Valid wiretap warrant/FISA order
    - Prior permission of 'party to communication'
    - To identify a source of electronic interference; or
    - 'Provider' of electronic communications service and
        - necessary to render service or
        - protection of rights/property of the provider
            - Fraud *against* instead of *using* the phone company
- Exceptions to prohibition on distribution
    - No knowledge that content was obtained illegally

Trap & Trace

- 18 USC 3121
  - Captures to/from/when with phone calls
  - Has been extended to email & packets
    - Routing information
  - More permissive than wiretaps
    - Provider exception
      - To protect users/provider/connected networks from fraud
      - Testing/maintenance
      - Billing
    - Or with warrant/court order/subpoena

Stored Communications Act

- 18 USC 2701- Stored Communications Act
  - Protects electronic communications while in transitory or long-term storage
    - Very transitory
    - Exceptions:
      - Intended recipient or sender (or with their consent)
      - Provider of 'electronic communications service'
        - No restrictions on their use- kinda
      - Valid court order/warrant

Computer Fraud And Abuse Act

- 18 USC 1030- Computer Fraud and Abuse Act
  - Protects most Internet- connected computers from intentional unauthorized access or exceeding granted access
    - Requires fraudulent intent or damage

More Fed laws

- 18 USC 1029
  - Prohibits counterfeiting or unauthorized use of 'access devices'
    - 'Access Device' is mechanical, electronic or logical object to gain access
- 4th Amendment of the U.S. Constitution
  - prohibits unreasonable searches or seizures by State actors
- DMCA (Digital Millennium Copyright Act)
  - Prohibits breaking of 'access controls' on copyrighted material

More relevant law

- State laws on the above topics
  - Often mirror Federal laws
  - Some interesting wrinkles (wiretap law as example)
- Common law torts
  - Nuisance
  - Slander/Libel
  - Intrusion into seclusion

Botnet Research Methods

- Capture
  - Active (go out and get malware)
    - Actual (use vulnerable browser/application)
    - Simulated (use tool that mimics vulnerable app)
    - FTP (go to malware repository)
  - Passive (let it come to you)
    - Honeypot/net
    - Collection from infected end-users

Active capture- legal issues

- Misconfigured acquisition tool/application causing damage to innocents
  - 1030 violation
  - Nuisance tort
- Downloading from malware repository
  - If in violation of site terms of service, 1030/contract claims

Passive Capture- legal issues

- Honeypot/net
  - Possible nuisance if net is staging ground
- End-user collection
  - Without permission-
  - 1030 unlawful access
  - 2511 if live capture of packets obtained
  - 2701 if stored communications obtained

Testing of malware- issues

- Reverse engineering/static analysis
  - Is the malware protected by copyright/DMCA?
- Sandbox/dynamic analysis
  - Potential nuisance if sandbox insecurely connected to outside world

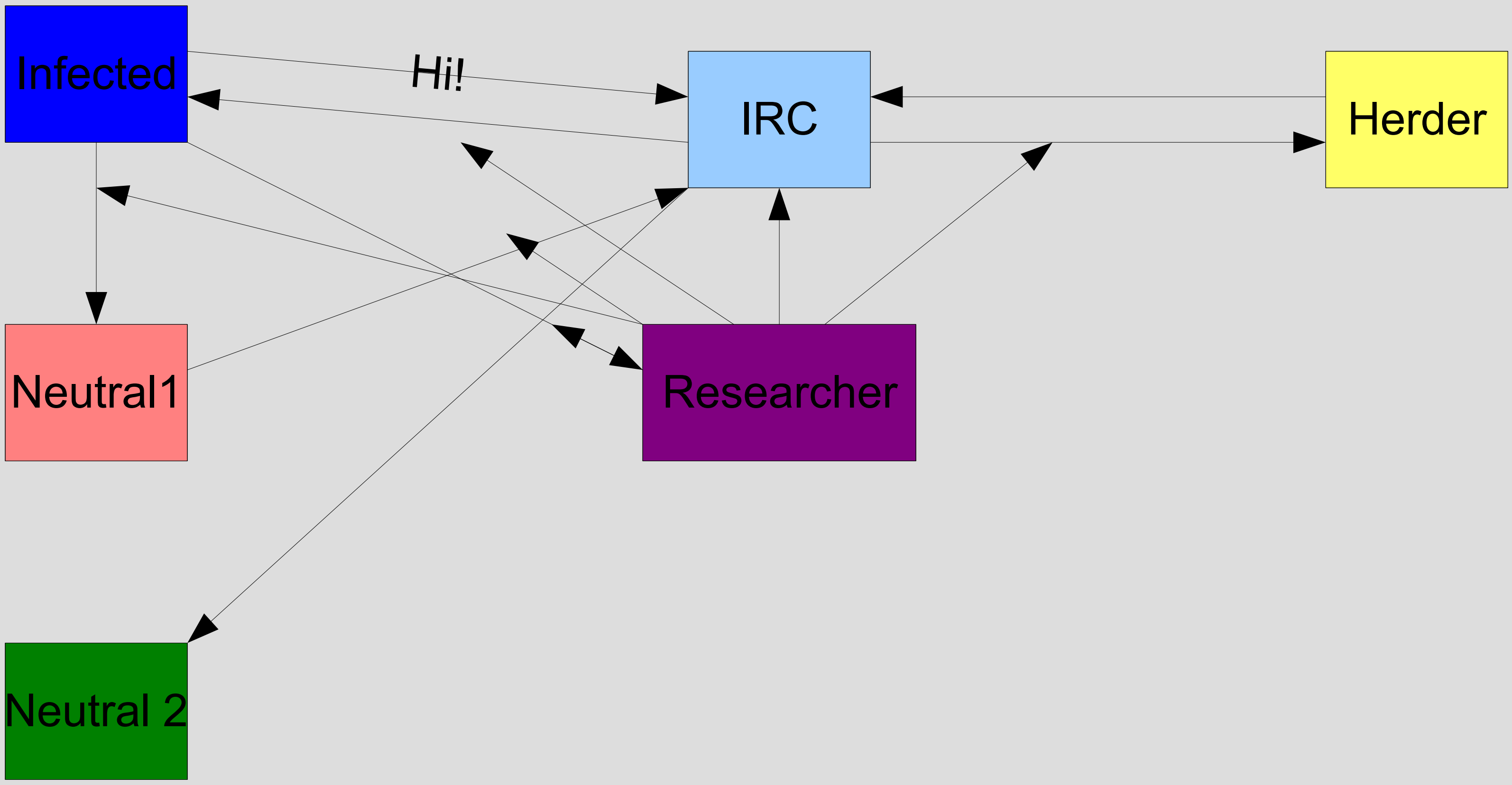
Publication legal issues

- Libel/slander claims
  - Negative, untrue statement of product
- Trade secret
  - If vendor has disclosed 'controlled' secrets
- 2511 'divulgement'
    - illegal interception and content is revealed

Monitoring of herders

- Logging onto herder IRC server to get info
  - Passive monitoring
    - Either listening between infected machine and herder or spoofing infected PC
  - Active monitoring
    - Poking around in the IRC server
- Sniffing traffic between bot & control channel
- What if herder is using 'mixed' server?
  - innocent and illicit traffic together

Insert crappy schematic



Issues of standing

- Unlikely that actual criminals will raise the issue
  - either civilly or criminally
- But you're not off the hook yet
  - Innocent traffic & users may complain
    - and sue
- Legal and illegal sites may not identify themselves

Researcher Hypo

- University researcher implements honeynet
  - Assumes all incoming traffic is illicit
    - And thus capture/storage/publication OK
  - Gets misrouted innocent traffic
    - Due to own error
    - Due to sender's error
    - Due to third party error
  - Makes traffic content available
  - Is in 2-party consent state

Is our researcher in trouble?

- Inadvertent acquisition is not wiretapping
  - But it's an affirmative defense only
  - If it's not, they're in trouble
    - Can't raise the 'provider' defense, as honeypot not related to protecting their network
    - Disclosure not related to protecting their own network
  - What about consent?
    - Receiver granted consent, so Feds are ok
    - State can get interested
      - As example- PA law- *all* parties must agree or
      - Prior agreement
      - in writing
      - Verified by Attorney General's office or DA's office

Botnet Defense

- Passive monitoring/defenses
  - IDS on own network
  - Or client's network
    - with permission and within scope
- Server side monitoring
  - When you discover a control server
    - Live or static investigation

Botnet Defense, contuned

- Takedown/Disruption
  - Pull the plug/null route/
    - Ok, if...
      - it's yours
      - you have permission
        - Actual permission
        - 'constructive' permission
  - DNS poisoning
    - Contract between herder & DNS provider
- More 'macho' responses
  - Counter-attack
    - Self-defense may be no defense at all...

IT defender Hypothetical

- End-user IT defenders
  - Get unfriendly traffic from botnet
  - Actively monitor incoming traffic
  - Gets upstream provider to dump traffic
- ISP defenders
  - Most traffic to and from their own clients
  - One or more clients being attacked
  - Actively monitor incoming/outgoing traffic
  - Dumps traffic, disconnects infected hosts

Hypo outcome

- End user defender-
  - Has permission to monitor own traffic
    - Employee contracts
  - Dumping traffic OK
    - Provided that it is either
      - True
      - good-faith based on evidence
- ISP defender
  - May have permission to monitor own traffic
    - TOS
    - Or can use 'prevent fraud' clause
  - Dumping traffic
    - Contract issue between users and ISP

Take-aways

- To protect yourself-
  - Write monitoring clauses in contracts with clients
  - Seek to avoid monitoring innocent traffic
  - Routing metadata less protected than content of communications
  - Stored communications protected differently
- Counterattacks are stupid
- Feel free to contact me- (or hire me)
  - lex@successfulseasons.com