What's worse, Cops at the door or a script kiddie at the mail gateway?

The law and law enforcement as attacker

Alex Muentz, Esq.
Pumpcon 2006

Disclaimer

- This talk is not legal advice, but for educational and entertainment purposes
- I am a lawyer, but I'm not YOUR lawyer
- Individual jurisdictions have subtly different rules. Contact local counsel if you're not from around here

Overview

- Why compare legal methods to that of illegitimate attackers?
- Understanding the types of 'attacks'
- What can I do to protect myself, my organization and my users?

Legal methods as attacks

- Often similar aims
- Shutdown
  - DOS attack or injunction
- Information
  - Database/file server intrusion or subpoena
- Similar response type
- Mitigation & Cleanup
  - Destructive intrusion or search warrant
- Reactive
  - Patch party or subpoena
- Proactive
  - IT or internal audit

Search Warrants

- “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”
  - Fourth Amendment, U.S. Constitution

Search Warrants, cont.

- Warrant requires:
  - Neutral Judicial Officer who finds sufficient
  - Probable cause that crime occurred, persons named (in warrant) are responsible or evidence is within place to be searched
  - Signed, written affidavit by LEO attesting to probable cause above
  - Particularity of items to be seized and area to be searched

Attack profile of the Search Warrant

- Noisy, destructive and messy
  - Little or no warning
    - No-knock vs knock warrants
  - NO immediate defenses
  - “Unintentional” collateral damage to obtain additional information
  - Scope of search can expand
    - 'Any relevant container' for named items
    - Plain view rule

Defenses to the Search Warrant

- IT Defenses
  - Multiple site data and systems backup
- Legal Defenses
  - Minimizing damage
      - Passive vs helpful
      - Don't get in the way
      - Shut the fuck up.
  - Attacking the warrant, exclusionary rule
    - Probable cause
      - Leon good faith exception to invalid warrant
    - Specificity of warrant

Warrantless Searches (an aside)

- Require probable cause
  - With notable exceptions
    - Search incident to lawful arrest
    - Automobile searches
    - Regulatory searches
      - Some new law – US v Arnold
        - Need reasonable suspicion to search laptop at border crossing
    - Exigent circumstances
    - “Terry” stops

Wiretaps

- Requires warrant under 18 U.S.C. §2510 et seq
  - Like warrant, must specify target and not capture innocent traffic
- CALEA (108 Stat. 4279)
  - Provider must enable the government to intercept targeted communications (and filter out innocent ones)
  - Concurrently with transmission
  - With valid warrant
  - Intercepted transmissions must be in a format transportable to government remote systems
    - Government may not specify provider equipment or specifications

Wiretap attack profile

- Stealthy and incriminating
  - Tapped upstream provider may not know of tap
  - Target not informed of tap until criminal discovery
- Defenses
  - IT
    - Strong encryption by party other than provider
      - Providers using encryption can be forced to divulge keys under CALEA §103(b)(3)
  - Legal
    - Attack warrant when revealed
      - Lack of probable cause, innocent communications

Subpoenas

- Two basic types
  - Subpoena Duces Tecum (SDT)
    - (Bring us stuff, or let us look at your stuff)
  - Subpoena ad testificandum
    - (Come and testify under oath)
- Who can issue them?
  - Grand Juries, regulatory agencies
  - Licensed Attorneys in many jurisdictions

Subpoenas, continued

- Dangerous
  - No right against self incrimination in civil/regulatory matters, must be invoked in criminal matters
- Limits on use
  - No undue burden or expense on recipient
  - No privileged material
  - Not for harassment or other improper purpose
- Enforcement
  - Civil contempt (fines and jail time until compliance)
  - Case dismissal
  - Jury instructions for missing evidence

Subpoena attack profile

- Intrusive, mysterious and dangerous
  - Reasonable time to respond
  - Can force you to admit incriminating facts
  - Mystery is actual purpose behind subpoena
    - (Am I the target or a witness?)
    - Do I fight or give them what they want?

Subpoena Defenses

- IT Defenses
  - Mitigation
    - Easily searched indexes of all electronic documents in enterprise
    - Clear and followed data retention policy
  - Stonewalling
    - Compartmentalization
    - Black holes
- Legal Defenses
  - Motion to Quash
    - Burden, Privilege, Trade secret
  - Protective Order
    - Limiting subpoena

Subpoena miscellaneous

- Encryption keys and passwords might not be protected
- But 'Providers of electronic communication service' may only disclose content of messages
  - With valid warrant (probable cause) to law enforcement (18 U.S.C. § 2703 (c)(1)(A)
  - With court order for customer records

Discovery Requests

- Requires filed litigation
  - Works like subpoena against parties to suit
  - Difference: destruction of evidence has nasty consequences
    - Sanctions to counsel
    - “Adverse Inference” instructions
- Defenses
  - Legal, mostly
    - Opposing discovery order
    - Burying 'smoking gun' in haystack of irrelevant info

Fun with transitive trust

- If B & C share datum i
  - Security of i depends on the weaker of B&C from attacker A's point of view
    - e.g. B has weaker security but A has an inside person at C
- Think of business data sharing as a network
  - Willingness to defend data is security
  - Different willingness to defend same data based upon requester
  - Can't get what you want from A? Figure out who else has that info and hit them

Transitive fun, continued

- New Jersey v Ceres (2005)
  - 'Perverted Justice' method to acquire screen-name
  - Subpoena AOL to get billing records and recorded chat logs
    - AOL more willing to give out subscriber info to LEO than civil parties
- Apple v Does (2005)
  - Apple Computer files trade secret suit against John Doe defendants
  - Subpoenas several owners of Apple discussion pages
  - Subpoenas ISP for email to owners
    - Owner defends on Stored Communications Act warrant requirement for email- to be determined by Cal. App Court.

Defending transitive attacks

- Know what information is shared with other organizations
  - Get agreements to alert you quickly- before they must deliver information
  - Intervene quickly and aggressively as party in interest
- Know what information is important, and what isn't
  - Can you keep sensitive information in-house?

Questions?

troll@dfire.org