

Protecting your IT infrastructure from Legal attacks:
Subpoenas, Warrants and Transitive Attacks

Alexander Muentz, Esq.
Defcon 15

- I am a lawyer, but not *your* lawyer
- The topics presented reflect my personal views and are not necessarily those of ONSITE³
- This talk is not legal advice, but for educational and entertainment purposes
- This field of law is in flux. What is good law today may not be next month
- Local laws vary.

Using the preparation/attack/response model

Types of attacks

What can I do to protect myself, my organization and my users?

- Similar aims
- Shutdown
 - Injunction
 - DOS attack
- Information
 - Database intrusion
 - Subpoena
- Similar precautions
- Good offsite backups
 - Destructive search warrant execution
 - Natural disaster
- Strong searching & archiving solution
 - Good for responding to discovery order
 - Useful for preventing redundant storage

- Search Warrants
- Subpoenas
- Discovery
- Wiretaps
- Transitive trust attacks

- “The rights 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

- **Warrant requires:**
 - Neutral Judicial Officer, who determines that
 - Probable cause that a
 - Crime occurred, and that
 - Persons named and/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.
- **Warrant allows-**
 - The items named in the warrant
 - Seizure of contraband, evidence, fruits and instrumentalities of crime found during search
 - For computers 'containing' the above, the seizure of the data or the computer (LEO's discretion)

- Noisy and destructive
 - Minimal warning
 - No-knock vs knock warrants
 - NO immediate defenses
 - You can't make it better
 - You can make it worse
 - “Unintentional” collateral damage to obtain additional information or to expand scope of search

- IT defences
 - Multiple site data and systems backup
 - Preferably in multiple jurisdictions
 - Automatic failover useful as well.
- Legal defences
 - Minimizing damage during the warrant execution
 - Helpful vs Passive
 - DO NOT INTERFERE
 - Shut the fuck up
- Cleaning up afterwards
 - Legal-Excluding evidence found in an invalid warrant (*Leon* rule)
 - IT- Cut over to alternate site or restore from backup to new boxen

- Generally require probable cause
 - Exceptions
 - Search incident to lawful arrest
 - Automobile searches
 - Regulatory searches (border crossing, airports)
 - ◆ *U.S. v Arnold* (need reasonable suspicion to search contents of laptop at border crossing)
 - Exigent circumstances
 - ◆ *U.S. v Heckencamp* (IT staffer can intrude into an attacker's PC to determine source of attack without violating 4th Amendment, and presumably 18 U.S.C. 1030)

- More exceptions
 - Third party searches
 - U.S. v Steiger (Turkish 'hacker' sends proof of child porn on Steiger's computer to local law enforcement)
 - Permissive Searches
 - U.S. v Andrus (Dad grants LEO access to son's PC, even though dad does not use or have password to computer; enough for LEO to assume Dad had authority to grant access)

- Requires warrant under 18 USC §2510 *et seq*
 - *Must specify target and not capture innocent traffic*
- *CALEA (Communications Assistance for Law Enforcement Act)*
 - *Provider must enable the government to intercept targeted communications (and filter out innocent ones)*
 - *Concurrent with transmission*
 - *Requires valid warrant*
 - *Intercepted transmissions must be in format 'transportable' to government*
 - *Government may not specify provider equipment or specifications*
 - *Issue with 'transportable'- is this merely compatible with remote monitoring or does it imply the ability to perform CALEA wiretaps w/o provider's knowledge?*

- **Stealthy and incriminating**
 - Tapped upstream may not know
 - Target will not know until after charged with crime.
- **Defenses**
 - IT
 - Strong encryption with limited distribution of private key
 - ◆ If ISP/Provider offers encryption, can be forced to divulge under CALEA §103(b)(3)
 - ◆ Grand Jury can subpoena keys from holders, but can't swear them to secrecy
 - ◆ National Security Letters limited to transactional information but do have gag orders 18 U.S.C. § 2709(c)
 - Legal
 - Attack warrant when revealed
 - ◆ If no PC, or other flaws, information can be suppressed
 - ◆ If innocent communications captured, possible civil remedies

- Court backed order for information
 - Issued by Attorneys, Grand Juries, Regulatory agencies
- Not a court order
 - Court order is order by a judge
 - Subpoena is order by an officer of court, and can be reviewed by a judge
- Two basic types
 - Subpoena Duces Tecum (SDT)
 - Bring us information or stuff, or let us look at stuff
 - Subpoena Ad Testificandum (SAT)
 - Come and testify under oath

- Not much protection
 - No right against self-incrimination in civil or regulatory issues
 - Right against self incrimination must be expressly invoked for criminal ones
- Limits on use
 - No undue burden or expense on recipient
 - Expense relative to size of controversy
 - Burden relative to alternate methods of getting same information
 - No privileged material
 - Not for harassment or improper purpose
- Enforcement
 - Civil contempt (fines or jail time until performance)

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

- 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
 - Limit subpoena

- Encryption keys and passwords might not be protected from disclosure
- But content of messages held by 'providers' may be protected
 - With valid warrant by law enforcement (18 U.S.C. § 2703(c)(1)(A))
 - With valid court order for customer records

- Requires filed suit
 - Works like subpoena against parties to suit
 - Automatic disclosure required: FRCP 26(a)(1)(B)
 - Must disclose locations and types of Electronically Stored Information (ESI)
 - ◆ Can protect from actual delivery if undue burden or cost (26(b)(2)(B))
 - Can supplement with additional orders against parties
 - Must be in format used by your organization (not Klingon)
 - Can also subpoena third parties for responsive information
 - Destruction of evidence once suit likely has bad consequences
 - Sanctions to counsel
 - Adverse inference instructions
 - Dismissal of claims

- Slow, expensive bleeding
 - E-discovery can get expensive and time consuming
 - This used to be the 'Third Rail' of litigation
 - Would be used to unnecessarily increase lawsuit costs
 - Old rules patchwork and unclear
 - December 2006 amendments
 - Rules clarified somewhat
 - Mandatory disclosure
 - Still expensive, and chance for really expensive errors
 - ◆ Duty to preserve may also be a duty to collect (Torrentspy)

- IT Defenses
 - Ability to quickly, efficiently and completely
 - Locate & retrieve responsive information
 - Determine cost of burdensome recoveries
 - Determine privilege
 - Archival/indexing solutions
 - Preserve responsive information
 - Document retention and destruction policies
 - Enforced & Rational
 - No loopholes

- Legal Defenses

- Opposing discovery order

- Showing costs and burden believably

- ◆ Colombia v Bunnell-(Torrentspy)- burden not shown

- Drinking from the fire hose

- ◆ Burying 'smoking gun' in haystack of responsive but useless information

- IT & Legal team effort
 - Pre- discovery
 - IT can quantify effort to get 'inaccessible' information
 - Legal can use this information to restrict or eliminate duty to turn over
 - During discovery
 - IT can assist with specifying incoming and outgoing discovery
 - Legal can force compatibility with other side
 - Counter-attack
 - A savvy IT person can help at the Rule 26 conference
 - ◆ Determine if other side is fudging
- When IT & Legal don't work well together
 - IT misunderstands Legal's needs
 - Risk of sanctions
 - Legal misunderstands IT's needs
 - Overly broad litigation holds
 - 'Death Spiral'

- Attacker probes for weakest link in chain of trust
- If B & C share datum i
 - Control 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 inside person at C
 - If B is less willing than C to fight to keep i secret
- Think of organizational data as a network
 - Willingness to defend data asset is security
 - Different willingness to defend same secret based upon requester
 - Rebuffed by B? go to C and ask

- New Jersey v Ceres (2005)
 - 'Perverted Justice' method acquires screen name and incriminatory chat
 - Subpoena to AOL maps screen name to IP address, login times, billing name and address
 - AOL more willing to give subscriber info to LEO than civil parties
- MySpace, Fyodor and GoDaddy
 - MySpace wants to get material off the net
 - two links in trust chain
 - ◆ Fyodor (interested in protecting material)
 - ◆ Domain Name Registrar (interested in avoiding litigation)
 - MySpace goes after weak link, and wins.

- 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?
- Defense agreements
 - Alert & defense (agree to pay for defense up to fixed amount)
 - Mutual defense (pay to defend other's data in your hands in exchange for same)

lex@successfullseasons.com

Thanks to:

Defcon organizers

Administrator's Office for the Third
Circuit Court of Appeals