So, you think you're hosting a Warez Ring...

What to do

What NOT to do

WAREZ Site: Accident?

- Accidental
  - Poorly maintained Windows system
  - SQL or SMB compromise
  - Helpful response from user
- Intentional
  - Well maintained, secure Linux system
  - Evasive user response.

Your guy comes to you...

- Normal intrusion detection
- Network flow monitoring
- Not working on behalf of law enforcement

No Touch Rule

- The very next step
- Need to know basis
- Those not involved in the investigation:
  - Don’t poke, probe, prod
  - Don’t contact machine owner

“You make the call…”

- Phone call, not e-mail
- Prior relationship with management
- Prior relationship with law enforcement

Facilities Available

- A segregated stream
- A secure place to put the data
- A restricted place to do analysis
- A separate place for data backup
- Someone to pay attention to the stream

How big is big?

- libpcap file limit of size 2GB
- Video files frequently large
- Multiple streams of large file transfers
- Complete stream capture rare*

*more on this later

How much is enough?

- Collect over a variety of time frames
  - Weekends and 2am are very popular
- Start new streams frequently
  - Object: get beginning and ending
- Requires constant monitoring

There be Dragons....

- User privacy
- Contaminated evidence
- Convince management (and their lawyer)

A tricky balance

When is enough?

- Due care and consideration
- Due haste

What you KNOW…

- JUST enough to know the details
- Contents
  - more than one stream
  - more than one day
  - more than one participant

What you THINK you know…

- Recovered ASCII transmissions
- Any ASCII in the clear
- Make a professional judgement call

What you have to GUESS at…

- Who lies where in what food chain
  - Sometimes based on other sources
- Possible hints:
  - Everything outgoing
  - Many incoming, few outgoing
  - Fifty-fifty

Technical Specifications

- TCPdump and Ethereal are your friends!
- -nn flags and the –r –w –s 1518
- Replicate a port for sniffing
- Segregate specific traffic of interest

Some Limitations

- Disable all name/service lookups
  - Not relevant data, speeds things up
- Breaking files into useful chunks
  - Re-filtering TCPDump to ascii files
  - split dumpfiles by TCP streams
- Reassembly of archive file types
  - RAR

“The names have been changed….

- Jet Li’s “The One”
- “Wet T-Shirt Babes”
- GTA and Madden’05

…to protect the clueless.”

- Get the beginning/end of stream
- Text outsets
- Tools to recover (extract) payload