SÉCURITÉ.ORG

ENISA / CERT-CC

DDoS Mitigation & SP/LEO contacts

How do ISPs work internally and externally ?

Nicolas FISCHBACH
Senior Manager, Network Engineering Security, COLT Telecom
nico@securite.org - http://www.securite.org/nico/

COLT

TierX SPs' organisation

- SPs range from “one man show” to large int'l operations
- AUP and telco&SP license define/restrict the scope of investigation/”debug” allowed
- Various groups are usually involved
  - Network Operations
    - NOC
    - Abuse
    - Security Operations (if not dedicated to MS)
  - Network Engineering
    - Network team
    - Security team
- What's the size of those teams ?
- What can they do / what kind of access do they have ?

Available data

- Administrative
  - Public RIR data
  - Internal RIR/IP allocation data
  - Customer profiles
- AAA
  - AAA from dial-in/*DSL users/portals
- Traffic data
  - Bandwidth reports
  - Netflow tele-metry data (“headers” only)
  - ACLs logs
- Data you and LEO would love to have
  - Full packet dumps (DPI)
  - MITM/stepping stones to fiddle with the client/server
  - The malware

Mitigation information sharing

- **Internally**
  - **99% of DDoS attacks handled by NetOps**
  - **A few escalations to Engineering**
    - **Large attacks impacting IP/MPLS core backbone**
    - **High profile customer**
  - **Abuse team to convince customer to share malware?**

- **Externally**
  - **Limited information sharing with vetted groups**
    - **Because this data is for mitigation, not prosecution**
    - **Trust model with known peers**
    - **Very limited leaks**
  - **With LEO: "Go by the book"**
    - **Internal Legal&Regulatory group involvement**
    - **"Confidential Informant" status ?**
    - **Slow process vs fast moving attack(er)s**
    - **Teaching the LEO about technology 101**
    - **The Internet vs int'l borders**
    - **Works best with long lasting "attacks"**

What's going to change (maybe)

- **EU Data Retention**
  - **(Mostly) well defined interfaces and policies**
- **Push for LI (Lawful Intercept)**
  - **Up to now mostly TDM/PSTN Voice only**
  - **Some countries already have IP/Data LI laws**
  - **Most EU countries "working on it"**
- **A challenge for large int'l telco/SPs**
  - **One LIDR Ops team ? Is this "legal" ?**
  - **The DDoS/malware fighter is usually "hiding"**
    - **Willing to help, but not officially**
    - **Usually bypassing the companies' rules**
    - **"Playing" with customer traffic**
    - **May loose his job if there's a leak**
- **DDoS are no news to SPs. Don't forget other threats**
- **What's the business case of all this ?**