DDOS – Anatomy of an Attack
OVERVIEW

- Definition
- Tools
- Notice
- Symptoms – Identification
- Composition of Attack
**Definition**

Distributed Denial of Service (DDOS)

Wikipedia - Is an attempt to make a computer or network resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of the concerted efforts of a person, or multiple people to prevent an Internet site or service from functioning efficiently or at all, temporarily or indefinitely.

DDOS as a form of hacktivism – activism + hacking **


** Verizon 2012 Data Breach Report – 58% of data breaches attributed to activism, 81% of all reported breaches caused by hacking.**
Recent Targets – 2012
LOIC – Low Orbit Ion Cannon

- An application developed by 4Chan-affiliated hackers designed to—when used en masse by thousands of anonymous users—launch Distributed Denial of Service (DDoS) attacks on websites.

- Windows version has “hive-mind” feature that allows you to point your local copy to a IRC server allowing for others to control at what site all LOIC clients are aimed. –Voluntary participation in a DDOS.

- Little to no risk of being caught –difficult to prove responsibility.

- Browser version – runs in any browser, on any platform (including SmartPhones).
LOIC

JS LOIC

No need to download, install or setup anything - just click the button, sit and enjoy the show.

Step 1. Select your target:
URL: https://www.paypal.com:443/
For current target see: http://anonsops.net/

Step 2. Ready?
IMMA CHARGING MAH LAZER

Optional Options
Requests per second: 10
Append message:

Attack status:
Requested: 0
Succeeded: 0
Failed: 0

We need your help in support of wikileaks leave this page firing as long as you can. Don’t worry if requests show as failed.
Intelligence Before, During, and After

- E-Mail
- Public Claims of Responsibility
- Political Message
- Law Enforcement
- Security Underground Network
- Other similar businesses/entities
Response

- Limit embryonic connections
- Logically move web servers, assign new temporary URL's
- Install equipment for better control management
- Block foreign source IP’s - upstream
- Design for DDOS resilience – Web App firewalls, locally controlled Gateways
- SaaS hosting or security solutions
Where Does Incident Response Fit in DR?
Security Incident Response Planning
Take Aways

- Plan, plan plan…test your plan…plan some more.
- Foster relationships with other agencies/departments, your service providers, and support organizations.
- Incident Post Mortem
Questions?