

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.

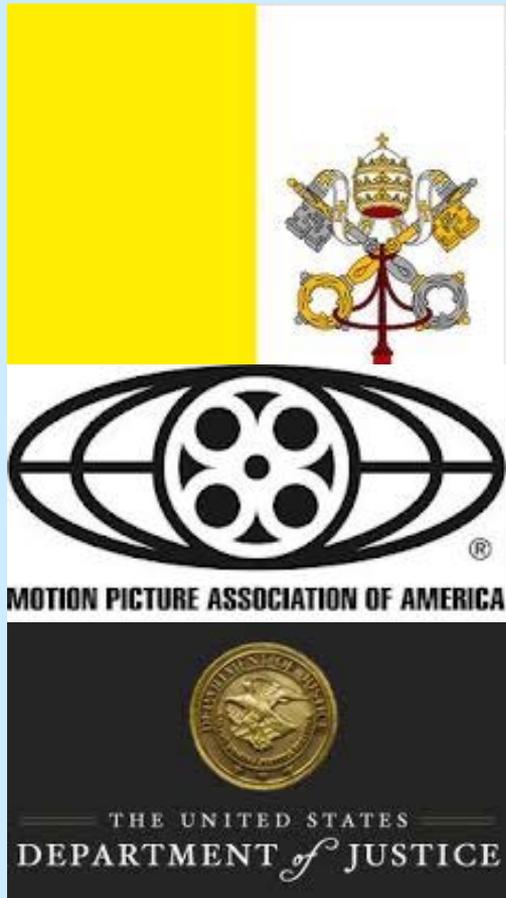
DDOS as a form of hacktivism – activism + hacking **

P.A. Taylor and T. Jordan, 2004. *Hacktivism and Cyber Wars, Rebels with a Cause* – “Hacktivism is activism gone electronic”

** Verizon 2012 Data Breach Report – 58% of data breaches attributed to activism, 81% of all reported breaches caused by hacking.



Recent Targets – 2012



A screenshot of a web browser displaying a PCMag article titled "DDoS Attacks on Financial Services Firms Explode". The article is by Damon Poeter, dated April 11, 2012. The main text reads: "Somebody is going after the Web infrastructure of financial services firms in a big way. Distributed denial of service (DDoS) attacks aimed at such companies serviced by Prolexic increased threefold, the firm said." The article includes social media sharing options for Facebook, Twitter, LinkedIn, and Digg. To the right of the article is an advertisement for an IBM System x Express server featuring Intel Xeon processors. The browser's address bar shows the URL: http://www.pcmag.com/article2/0,2817,2402898,00.asp. The Windows taskbar at the bottom shows the time as 3:01 PM on 4/11/2012.



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:

For current target see: <http://anonops.net/>

Step 2. Ready?

Optional. Options

Requests per second:

Append message:

Attack status:

Requested:

0

Succeeded:

0

Failed:

0

We need your help in support of [wikileaks](http://wikileaks.org) 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**

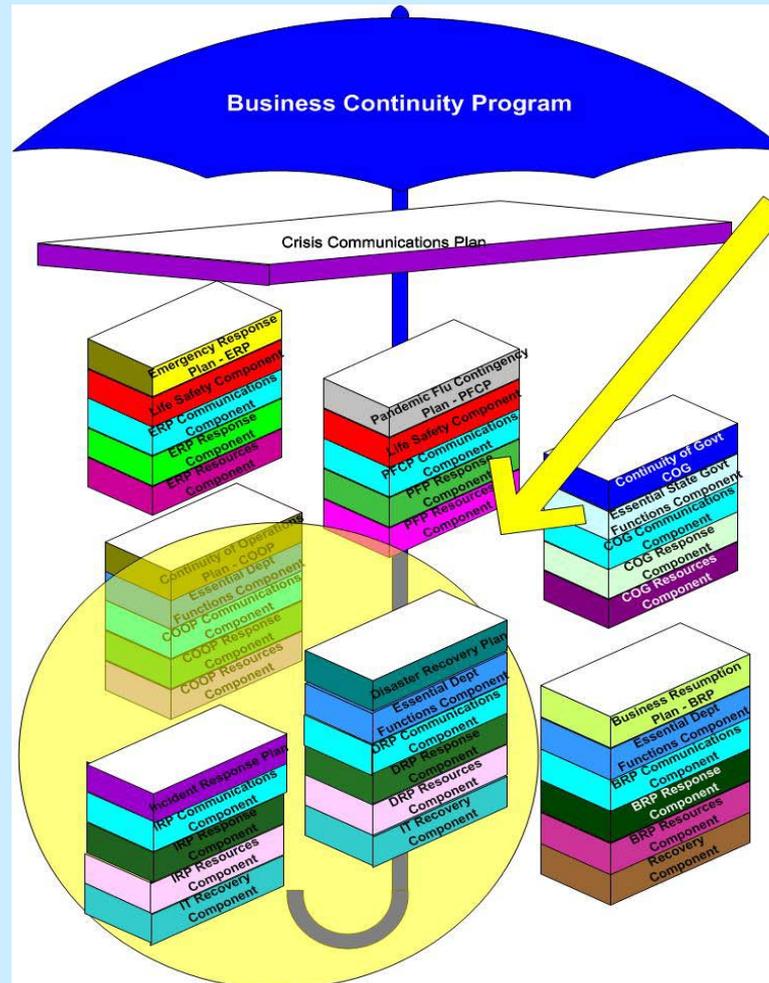


Response

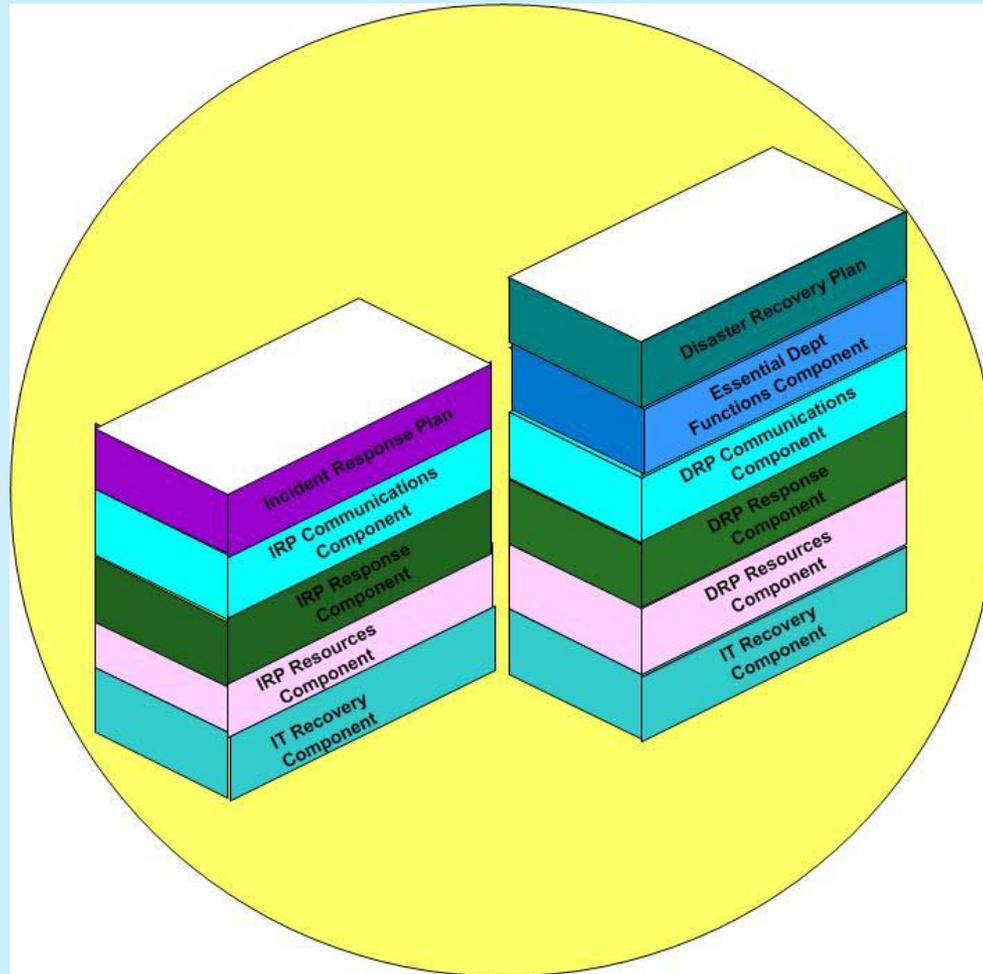
- **Limit embryonic connections**
- **Logically move web servers, assign new temporary URL's**
- **Install equipment for better control management**
- **Block foreign source IP's - upstream**
- **Design for DDOS resilience – Web App firewalls, locally controlled Gateways**
- **SaaS hosting or security 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?

