In the News....

Anonymous dupes users into joining Megaupload attack

Daunell Butt

CS466: Computer Security

January 30, 2012

Meet the Players

- "File Hosting" Service

Meet the Players

- "File Hosting" Service
- Large web site that allows distribution of illegal media

Meet the Players

- "File Hosting" Service
- Large web site that allows distribution of illegal media
- Headquarters in Hong Kong but servers world wide

Meet the Players

Meet the Players

- Motion Picture Association of America MPAA
- Recording Industry Association of America RIAA
- Universal Music

Shut down of Megaupload

Shut down of Megaupload

- 4 of 7 people indicted were arrested

Shut down of Megaupload

- 4 of 7 people indicted were arrested
- Kim Dotcom, the founder was one of the 4 arrested

Meet the Instigator

ENTER .... ANONYMOUS!

Meet the Instigator

ENTER .... ANONYMOUS!

- HACTIVIST Group aka hacking activists

Meet the Instigator

ENTER .... ANONYMOUS!

- HACTIVIST Group aka hacking activists
- Within hours a DDoS was Launched in retaliation

Meet the Instigator

ENTER .... ANONYMOUS!

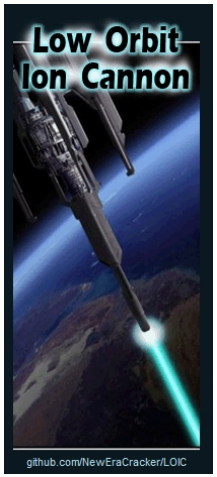
- HACTIVIST Group aka hacking activists
- Within hours a DDoS was Launched in retaliation
- Distributed Denial-of-Service

Meet the Instigator

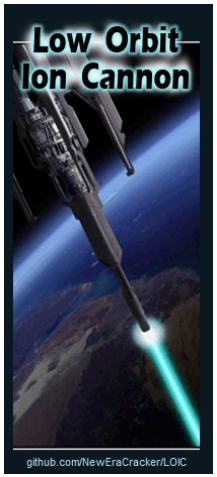
ENTER .... ANONYMOUS!

- HACTIVIST Group aka hacking activists
- Within hours a DDoS was Launched in retaliation
- Distributed Denial-of-Service
- Here is how they did it....

Low Orbit Ion Cannon LOIC

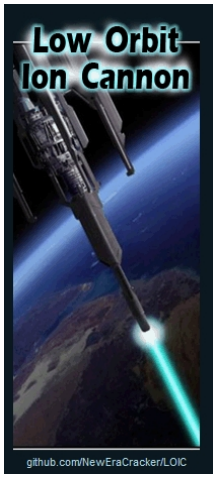


Low Orbit Ion Cannon LOIC



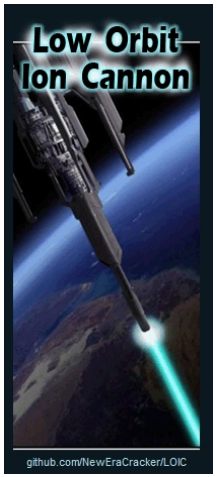
- Open source network stress testing application

Low Orbit Ion Cannon LOIC



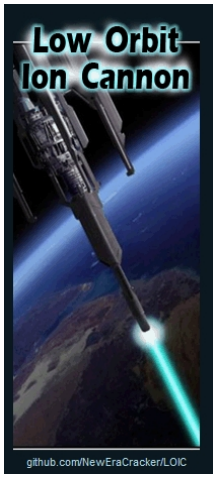
- Open source network stress testing application
- Named after a fictitious weapon from the Command and Conquer video game

Low Orbit Ion Cannon LOIC



- Open source network stress testing application
- Named after a fictitious weapon from the Command and Conquer video game
- Sends a deluge of packets to server

Low Orbit Ion Cannon LOIC



- Open source network stress testing application
- Named after a fictitious weapon from the Command and Conquer video game
- Sends a deluge of packets to server
- Used in Denial-of-Service attacks

The TWIST

- new way to instigate Distributed part of attack

The TWIST

- new way to instigate Distributed part of attack

- Usually use botnet to launch DDoS - zombie computers

The TWIST

- new way to instigate Distributed part of attack

- Usually use botnet to launch DDoS - zombie computers
- Used a modified version of LOIC disguised as a website

The TWIST

- new way to instigate Distributed part of attack

- Usually use botnet to launch DDoS - zombie computers
- Used a modified version of LOIC disguised as a website
- Distributed innocent looking hyperlinks via Twitter, Facebook and Tumblr

The TWIST

- new way to instigate Distributed part of attack

- Usually use botnet to launch DDoS - zombie computers
- Used a modified version of LOIC disguised as a website
- Distributed innocent looking hyperlinks via Twitter, Facebook and Tumblr
- Once opened it launched an attack from user's computer

The TWIST

- new way to instigate Distributed part of attack

- Usually use botnet to launch DDoS - zombie computers
- Used a modified version of LOIC disguised as a website
- Distributed innocent looking hyperlinks via Twitter, Facebook and Tumblr
- Once opened it launched an attack from user's computer
- Note: neither the old down loadable version or the new in browser version hides users' identities

The TWIST

- new way to instigate Distributed part of attack

- Usually use botnet to launch DDoS - zombie computers
- Used a modified version of LOIC disguised as a website
- Distributed innocent looking hyperlinks via Twitter, Facebook and Tumblr
- Once opened it launched an attack from user's computer
- Note: neither the old down loadable version or the new in browser version hides users' identities
- 5635 people were confirmed to have launched LIOC

The TWIST

- new way to instigate Distributed part of attack

- Usually use botnet to launch DDoS - zombie computers
- Used a modified version of LOIC disguised as a website
- Distributed innocent looking hyperlinks via Twitter, Facebook and Tumblr
- Once opened it launched an attack from user's computer
- Note: neither the old down loadable version or the new in browser version hides users' identities
- 5635 people were confirmed to have launched LIOC
- Question is how many knew what they were doing and should all be held liable

The Result

Department of Justice, Universal Music,
Recording Industry Association of America (RIAA),
Motion Picture Association of America (MPAA)
were SHUT down

The Result

Department of Justice, Universal Music,
Recording Industry Association of America (RIAA),
Motion Picture Association of America (MPAA)
were SHUT down

- Availability GONE

Countermeasures

Countermeasures

- There are ways under development to limit this attack

Countermeasures

- There are ways under development to limit this attack
- Tarpit

Countermeasures

- There are ways under development to limit this attack
- Tarpit
- Shut down at IP or router

Countermeasures

- There are ways under development to limit this attack
- Tarpit
- Shut down at IP or router
- Harm - Availability only, Integrity and Confidentiality intact

Questions

Questions

- Besides commerce why is this kind of attack bad?

Questions

- Besides commerce why is this kind of attack bad?
- What is Anonymous trying to prove?

Questions

- Besides commerce why is this kind of attack bad?
- What is Anonymous trying to prove?
- Should the Justice Department have that much power?

Questions

- Besides commerce why is this kind of attack bad?
- What is Anonymous trying to prove?
- Should the Justice Department have that much power?
- How should copyrighted material be protected?

Where I found information

http://www.networkworld.com/news/2012/012012-anonymous-dupes-users-into-joining-255143.html
http://www.computerworld.com/s/article/9223557/
http://pastehtml.com/
http://en.wikipedia.org/wiki/ for some explanation of terms
http://www.justice.gov/
http://www.megaupload.com for picture of seized site