**Universidade Federal do Rio de Janeiro**

**Redes de Computadores I**

**Grupo:**

* **Lucas de Carvalho Gomes**
* **Marcos Seefelder**
* **Vinícius Campos**

**Tema: Negação de Serviço: DoS, DDoS e Botnets**

**Bibliografia**  
  
[1] $3 Million Reward Offered for International Cyber Criminal - FBI News Blog, 24 de fevereiro de 2015  
http://www.fbi.gov/news/news\_blog/3-million-reward-offered-for-international-cyber-criminal  
  
[2] Karl Thomas, The world’s most wanted hackers, 4 de maio de 2015. Obtido no site We Live Security. http://www.welivesecurity.com/2015/05/04/worlds-wanted-hackers/  
  
[3] SIMDA botnet down: 770,000 infected computers rescued, 21 de abril de 2015.  
http://searchsecurity.techtarget.com/news/4500244750/SIMDA-botnet-down-770000-infected-computers-rescued  
  
[4] U.S. Leads Multi-National Action Against GameOver Zeus Botnet and Cryptolocker Ransomware, Charges Botnet Administrator - FBI National Press Releases, 2 de junho de 2014.  
http://www.fbi.gov/news/pressrel/press-releases/u.s.-leads-multi-national-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware-charges-botnet-administrator  
  
[5] Rhiannon Williams, The biggest ever cyber attacks and security breaches - The Telegraph, 22 de maio de 2014  
http://www.telegraph.co.uk/technology/internet-security/10848707/The-biggest-ever-cyber-attacks-and-security-breaches.html  
  
[6] Avinash Kak, Lecture Notes on “Computer and Network Security” - Purdue University, 22 de abril de 2015 (52 págs.)  
https://engineering.purdue.edu/kak/compsec/NewLectures/Lecture29.pdf

[7] Eggheads: Eggdrop: Um dos primeiros sistemas de botnet pelo IRC, um tipo legal de botnet.  
http://www.eggheads.org/  
  
[8] Charity Engine  
http://www.charityengine.com/  
  
[9] Folding@Home (Stanford)  
http://folding.stanford.edu/  
  
[10] *Know your enemy: Tracking Botnets*  
http://www.honeynet.org/node/51  
  
[11] Ramneek Puri, Bot & Botnet: An Overview, agosto de 2003 (18 págs)  
http://www.sans.org/reading-room/whitepapers/malicious/bots-botnet-overview-1299  
  
[12] Maarten Vanhorenbeeck, Mobile botnets: an economic and technological assessment 7  
http://www.daemon.be/maarten/mobbot.html  
  
[13] Evan Cooke, Farnam Jahanian, Danny McPherson, The Zombie Roundup: Understanding, Detecting, and Disrupting Botnets  
https://www.usenix.org/legacy/event/sruti05/tech/full\_papers/cooke/cooke\_html/  
  
[14] Gunter Ollmann (Vice-presidente de Pesquisa da Damballa, Inc.), The Botnet vs. Malware Relationship (6 págs.)  
https://www.damballa.com/downloads/d\_pubs/WP%20Many-to-Many%20Botnet%20Relationships%20%282009-05-21%29.pdf  
  
[15] Gunter Ollmann (Vice-presidente de Pesquisa da Damballa, Inc.), Botnet Communication Topologies: Understanding the intricacies of botnet command-and-control (7 págs.) 10https://www.damballa.com/downloads/r\_pubs/WP%20Botnet%20Communications%20Primer%20%282009-06-04%29.pdf  
  
[16] Jelena Mirkovic, Janice Martin e Peter Reiher, A Taxonomy of DDoS Attack and DDoS Defense Mechanisms  
http://www.lasr.cs.ucla.edu/ddos/ucla\_tech\_report\_020018.pdf  
  
[17] Tao Peng, Christopher Leckie e Kotagiri Ramamohanarao, Proactively Detecting Distributed Denial of Service Attacks Using Source IP Address Monitoring  
http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.141.5038&rep=rep1&type=pdf  
  
[18] Emerson Alecrim, Ataques DoS (Denial of Service) e DDoS (Distributed DoS)  
http://www.infowester.com/ddos.php  
  
[19] Defeating DDoS Attacks, Cisco Guard DDoS Mitigation Appliances  
http://www.cisco.com/c/en/us/products/collateral/security/traffic-anomaly-detector-xt-5600a/prod\_white\_paper0900aecd8011e927.html  
  
[20] Verisign Distributed Denial of Service Trends Report: Issue 3 - 3rd Quarter 2014  
http://www.verisigninc.com/assets/report-ddos-trends-Q32014.pdf  
  
[21] Gunter Ollmann (Vice-presidente de Pesquisa da Damballa, Inc.), Understanding The Modern DDoS Threat  
https://www.damballa.com/downloads/r\_pubs/WP\_Understanding\_the\_Modern\_DDoS\_attack.pdf  
  
[22] Akash Mittal, Ajit Kumar Shrivastava, Manish Manoria, A Review of DDOS Attack and its Countermeasures in TCP Based Networks   
<http://airccse.org/journal/ijcses/papers/1111ijcses13.pdf>

[23] Wesley M. Eddy, Defenses Against TCP SYN Flood Attacks. Obtido em <http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_9-4/syn_flooding_attacks.html>

[24] *Request for Comments 4987 – Internet Engineering Task Force (IETF). Obtido em* <https://tools.ietf.org/html/rfc4987>

[25] *Smurf IP Denial of Service Attacks* - DIvisão CERT - Instituto de Engenharia de Software da Universidade Carnegie Mellon. Obtido em http://www.cert.org/historical/advisories/ca-1998-01.cfm?

[26] *DDoS Attacks* - Incapsula. Obtido em https://www.incapsula.com/ddos/ddos-attacks/

[27] <http://www.garykessler.net/library/ddos.html>

[28] David Cornell, *DNS Amplification Attacks* - OpenDNS Security Labs. Obtido em <https://labs.opendns.com/2014/03/17/dns-amplification-attacks/>

[29] Greg Lindsay, *DNSSEC and DNS Amplification Attacks* - Technet (Microsoft). Obtido em: <https://technet.microsoft.com/en-us/security/hh972393.aspx>

[30] Thijs Rozekrans, Javy de Koning, *Defending against DNS reflection amplification attacks*. Obtido em: https://www.nlnetlabs.nl/downloads/publications/report-rrl-dekoning-rozekrans.pdf

[31] UDP Flood - DDoS Attack Glossary - Incapsula. Obtido em https://www.incapsula.com/ddos/attack-glossary/udp-flood.html