DDOS protection solutions in Moldova in private, governmental and research and educational Networks.

MD-CERT

RENAM.

DDoS Mitigation in the NREN Environment Workshop

Alexandr Golubev

Agenda

1. Introduction
2. General Overview
3. Analyzing of potential DDOS targets.
4. DDOS Protection Tools and Services
5. AntiDDOS Overlay Initiative.
6. Conclusions
7. Questions

Introduction

- MD-CERT - CERT is a center of internet security expertise, located at the RENAM. We study internet security vulnerabilities, research long-term changes in networked systems, and develop information and training to help you improve security.

- Our Team started activity at 2006, thanking a NATO project that was targeted to set up CERT in Moldova, Ukraine and Belarus.

- RENAM - Research and Education National Association from Moldova is the largest ISP for R&E organizations from Moldova. RENAM Clients are the bigger Universities and Scientific centers from Moldova, Including State University, Technical University, Economy Academy and other with thousands of students, teachers and scientific staff

Currently there are 2 CERT in Moldova:

- MD-CERT that handles incidents in R&E network – www.cert.md
- CERT.GOV.MD is governmental CERT – http://cert.gov.md/

General Overview

Nowadays 90% of territory of Moldova is covered by Internet, that means that you can have internet access almost everywhere. We also have many free wi-fi access points in big cities and high speed internet connection even for home users.

This makes Internet resources accessible for most of citizens and network services, that’s why there are opened many internet shops, online delivery, online services and baking. However the number of online services is still very poor because of poor ebanking integration and low usage of online payment. The fact is that pay pall starts working in Moldova only 1 year ago…

Anyway the number of online services is growing up, that means that number of potential DDOS targets is also growing up.

fppt.com

Analising of potential DDOS targets

There are a group of internet resources that usually are in a risk group:

- eBanking Systems
- Payment Gateways
- News Portals
- E-Gov (governmental online services)
    - M-Pay
    - M-Sign
- Specific Governmental Institutions services.

fppt.com

DDOS protection Tools and Services

All these services from risk group potentially could be attacked because them are critical. Market of DDOS protection tools in Moldova is limited and can be listed below.

- It lab system integrator. The only one company that offers DDOS protection solutions. This is hardware solution based on blackhole rerouting.

- ISP offers DDOS protection, but in fact it does not work.

fppt.com

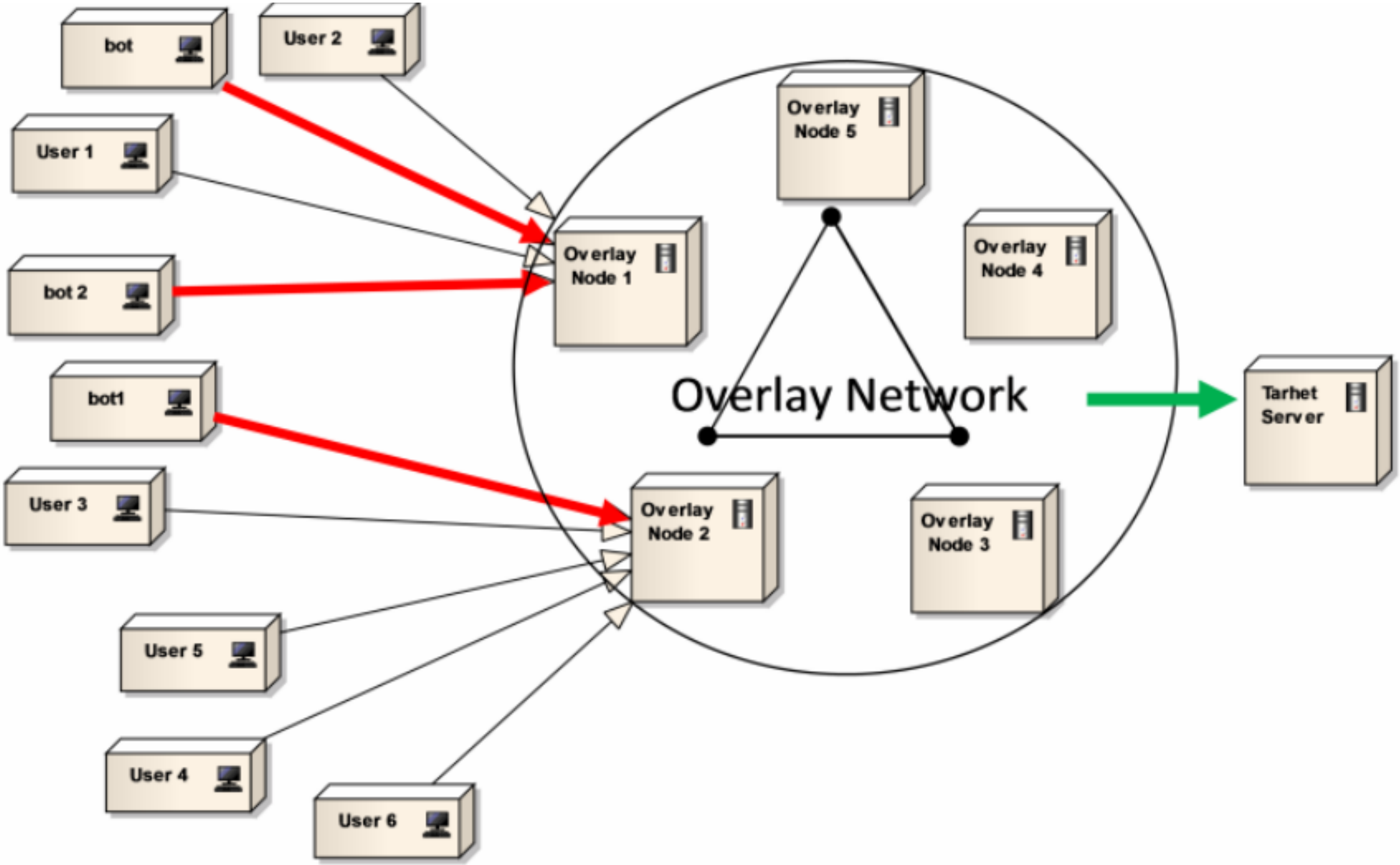
AntiDDOS Overlay Initiative

MD-CERT proposed an Innovation - Overlay Network – as a measure for defending against DDoS.

Overlay network is a global solution for solve DDOS problem for a big network, that allows to redirect and process an request of an legacy user in case if one of the nodes of overlay network is busy. Main idea of using overlay network as a measure for defending against botnets is to use the same tactics like is using by hackers.

fppt.com

Overlay – Main idea



DDOS Experiment

For test we used server where is hosted WebSite of medical Emergency (903) of Chisinau

- ASP.NET
- SQL Microsoft Sever 2008
- Windows 2003
- WEB SERVER IIS 6
- Intel Xenon 1.8 hz
- 1 Gb of RAM

fppt.com

DDOS Experiment Result

- Web site can serve about 1500 requests per minute.
- Minimal price for DDOS attack is about 50$ for 1000 bots per minute.
- Every bot can generate 3 request per second
- It means that server must be able to serve 181500 requests per minute

fppt.com

DDOS Experiment Conclusions

After these results we integrated a CAPTCHA for this web site. And test result were following:

- 5858 request per minute for this website
- It means that we need have about 30 nodes in our overlay network for cover this DDOS attack.

fppt.com

Questions

?