

anti DDOS network in Moldova

Alexandr Golubev
(E-mail: galex@renam.md)
RENAM Association

www.cert.md
www.renam.md



Advantages and disadvantages of creating an antiDDOS Network.

- **Overlay Network is the most powerful measure for defending against DDOS**
- **90% of territory of Moldova is covered by Internet**
- **Most servers and web services are hosted in the capital**
- **Moldova is a small country with a high speed national intranet**



There are a number of measures how Internet providers are trying to defend against DDOS:

- **Blackhole rerouting – redirecting bot requests to an unexciting ip address.**
- **Filtering and blocking by some conditions (for example using CAPTCHA «Completely Automated Public Turing test to tell Computers and Humans Apart»)**
- **Direct measures against the source of attacks. Such as blocking IP by country filter or using help from exiting CERT.**



Standard measures against DDoS attacks for an internet provider

- **Arbor Networks**
- **Cisco Systems, Inc.**
- **CloudShield Technologies**
- **Narus, Inc**

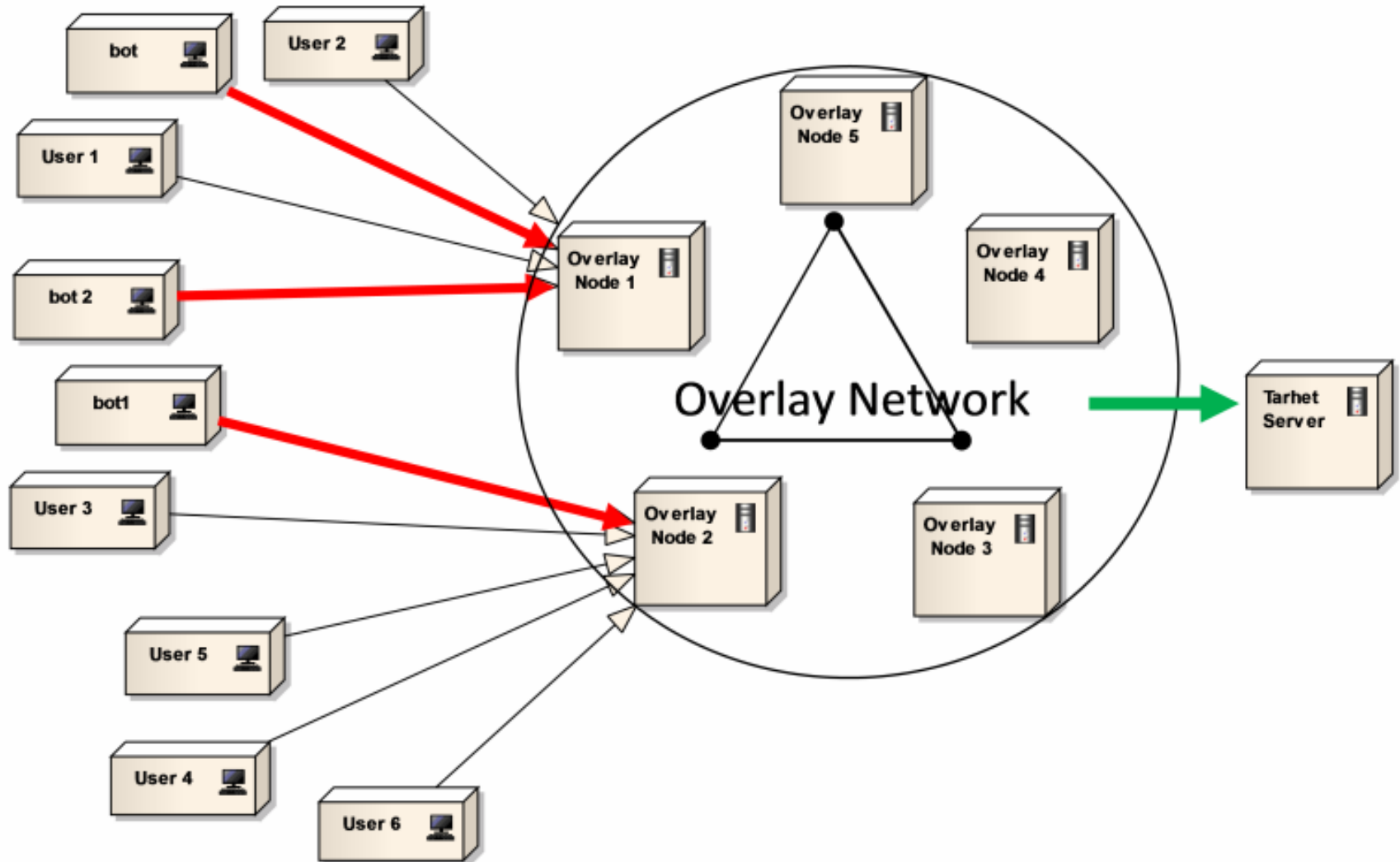


Overlay Network – as a measure for defending against DDoS

- **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.**

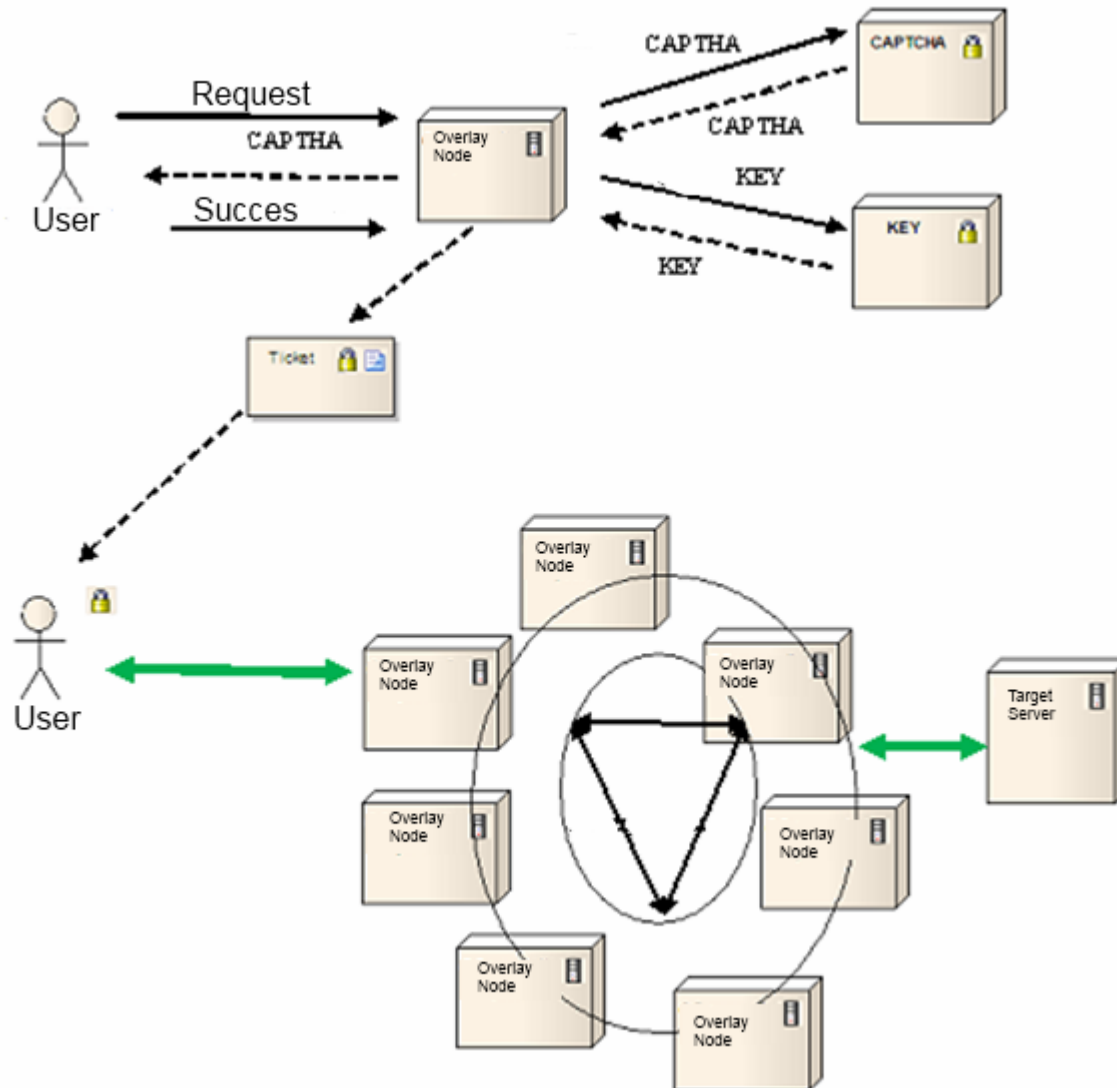
Creation of anti DDOS network in Moldova

Overlay Network



Creation of anti DDOS network in Moldova

Algorithm for defining an legacy User



Creation of anti DDOS network in Moldova

Test Results

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

Creation of anti DDOS network in Moldova

Test Results

- **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**

===== ВЗЯТО ИЗ ЖУРНАЛА "ХАКЕР", www.xakep.ru =====

[Заработок на DDoS-атаках]

DDoS-атаки - это очень прибыльное дело. Минимальная плата за DDoS-атаку в час - 40\$-50\$. И при том, что сервер не "крутой", который валить.

- **It means that server must be able to serve 181500 requests per minute**

Creation of anti DDOS network in Moldova

Test Results

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.

Integration of black lists and filtering methods:

- There is a request from one location(IP) more that 100 requests per minute
- CAPTCHA is filled with error for 10 times during 1 minute
- Entities in black list expire in 24 hours

After these modifications we recalculated number of nodes:

~3-5 nodes for this type of attacks.

Creation of anti DDOS network in Moldova



- **Main advantages of using of such overlay network:**
 - **Users can access every overlay node even one of the nodes is under attack.**
 - **Every node have possibility to identify legacy users**
 - **request of the user that passed the CAPTHCA are processed as secured.**
 - **There are possibility to increase number of nodes in your network.**
 - **One overlay network can offered defense against DDOS for many nodes.**

Creation of anti DDOS network in Moldova



- **This module can be used as for commercial purposes and for governmental national level.**
- **Information about black lists can be distributed for other security networks, that will help with fighting against botnets.**
- **Overlay network can be based also on such systems like PlanetLab and GRID.**
- **Nodes of the Overlay Network can be distributed by the region, but taking under consideration saving usability of web resources it is logicaly that the internet connection speed may be the same for all nodes.**