DDOS Analytics Tools Overview. Performance and Load network nodes testing.

Golubev Alexandr
RENAM
galex@renam.md

CS Danube (Cyber Security in Danube Region) project is part financed by the European Union from the START Danube Region Project Fund.

Agenda

1. Introduction
2. General Overview
3. DDOS Classification/Types
4. Analyzing of potential DDOS Aims.
5. Web Application Critical Resources.
6. DDOS Analytics Tools
7. AntiDDOS Overlay Initiative.
8. Conclusions
9. Questions

CS Danube (Cyber Security in Danube Region) project is part financed by the European Union from the START Danube Region Project Fund.

Introduction

- *Nowadays DDOS is one of the most powerful tools for intruders and hackers to make a real commercial profit.*
- *That causes creation many distributed DDOS Networks with online payment and distribution, which have its own billing system and plan configurable attack online.*
- *This makes DDOS one of the most dangerous attacks either for commercial and governmental sector.*
- *These attacks are usually started when potential victim is already overloaded and its stable work is critical, and could not be stopped quickly without losing a part of legitimate users.*

CS Danube (Cyber Security in Danube Region) project is part financed by the European Union from the START Danube Region Project Fund.

DDOS Classification/Types

- UDP Flood
- ICMP (Ping) Flood
- SYN Flood
- Ping of Death
- Slowloris
- NTP Amplification
- **HTTP Flood**
- Zero-day DDoS Attacks

Thanks to https://www.incapsula.com/ddos/ddos-attacks/

CS Danube (Cyber Security in Danube Region) project is part financed by the European Union from the START Danube Region Project Fund.

HTTP Flood

HTTP flood **DDoS** attack the attacker exploits seemingly-legitimate **HTTP GET or POST** requests to attack a web server or application.

HTTP floods do not use malformed packets, spoofing or reflection techniques, and require **less bandwidth** than other attacks to bring down the targeted site or server.

The attack is most effective when it forces the server or application to allocate the maximum resources possible in response to each **single request**.

CS Danube (Cyber Security in Danube Region) project is part financed by the European Union from the START Danube Region Project Fund.

Analyzing of potential DDOS Aims

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

-Sale systems.

-E-Banking Systems

-Payment Gateways

-News Portals

-Governmental online services

What is the common for these resources? This is critical infrastructure.

CS Danube (Cyber Security in Danube Region) project is part financed by the European Union from the START Danube Region Project Fund.

Web Application Critical Resources

"To understand how you can protect your applications you need to understand how intruder can crash it."

Here is a list of resources ordered by maximal loading:

1. Simple client side html pages – almost impossible to dos.
2. Statically servers side resources– no database connection
3. Servers side resources with database connection
4. Servers side resources with database connection and huge database request.

Intruder should know/analyze the application in order to know what to attack.

CS Danube (Cyber Security in Danube Region) project is part financed by the European Union from the START Danube Region Project Fund.

Web Application Critical Resources

What can be done by developer **before** DDOS Attack started:

1. Use unlimited resources – the simples one.
2. Use Captha.
3. Use Queues.
4. Do not allow huge requests for public access resources.
5. Build an alert system.
6. Load Testing!!!

CS Danube (Cyber Security in Danube Region) project is part financed by the European Union from the START Danube Region Project Fund.

Web Application Critical Resources

What can be done by developer **after** DDOS Attack started:

1. Ip filtering.
2. Manual Load Balancing.
3. Collect the logs.
4. Use alternative domains.

CS Danube (Cyber Security in Danube Region) project is part financed by the European Union from the START Danube Region Project Fund.

DDOS Analytics Tools

Wcat

Web Capacity Analysis Tool (WCAT) is a lightweight HTTP load generation tool primarily designed to measure the performance of a web server within a controlled environment. WCAT can simulate thousands of concurrent users making requests to a single web site or multiple web sites. The WCAT engine uses a simple script to define the set of HTTP requests to be played back to the web server. Extensibility is provided through plug-in DLLs and a standard, simple API.

CS Danube (Cyber Security in Danube Region) project is part financed by the European Union from the START Danube Region Project Fund.

DDOS Analytics Tools

Jmeter

Apache JMeter may be used to test performance both on static and dynamic resources (Webservices (SOAP/REST), Web dynamic languages - PHP, Java, ASP.NET, Files, etc. -, Java Objects, Data Bases and Queries, FTP Servers and more). It can be used to simulate a heavy load on a server, group of servers, network or object to test its strength or to analyze overall performance under different load types. You can use it to make a graphical analysis of performance or to test your server/script/object behavior under heavy concurrent load.

CS Danube (Cyber Security in Danube Region) project is part financed by the European Union from the START Danube Region Project Fund.

DDOS protection Tools and Services In Moldova

All these services from risk group potentially could be attacked because them are critical resources. 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.

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

CS Danube (Cyber Security in Danube Region) project is part financed by the European Union from the START Danube Region Project Fund.

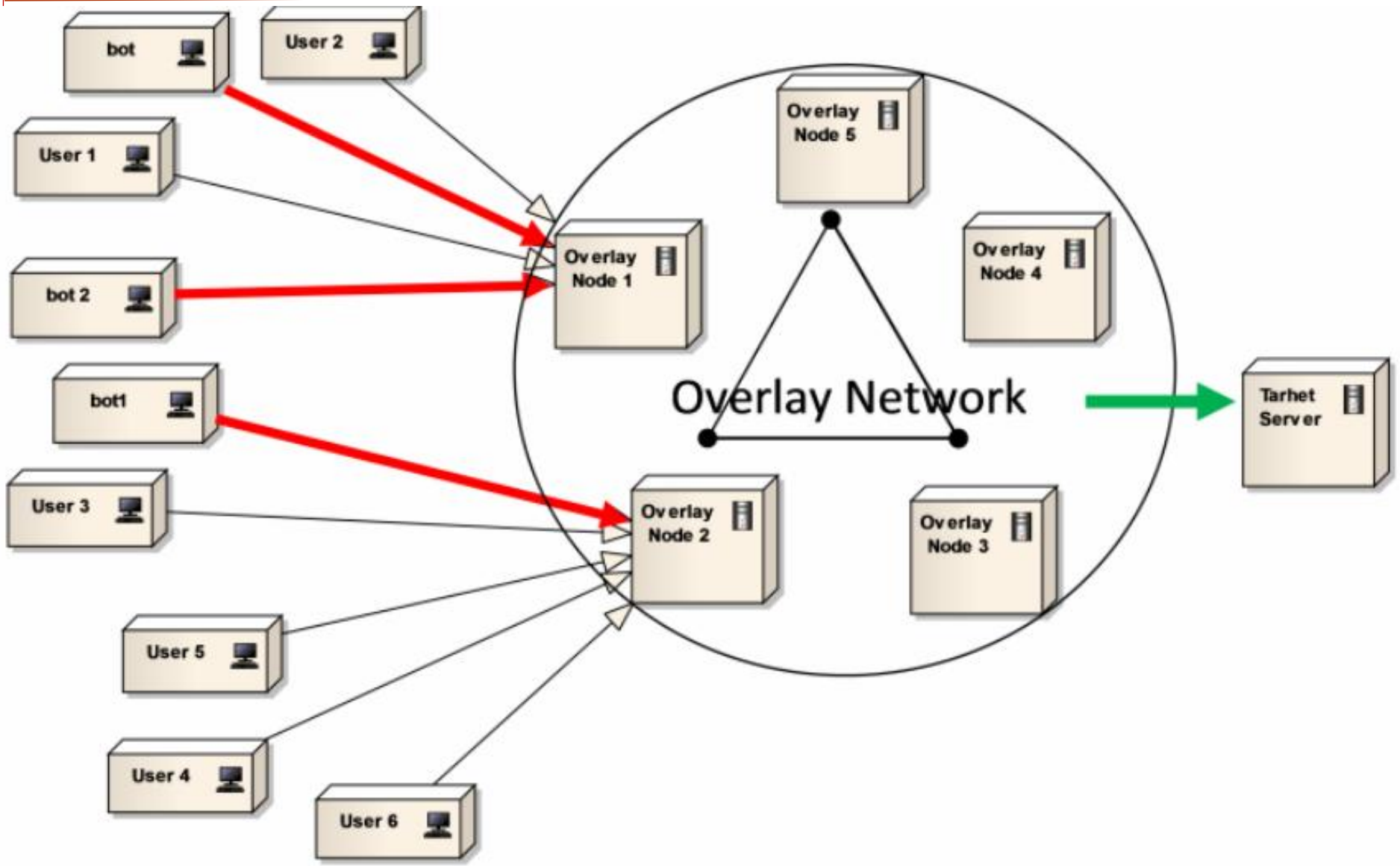
AntiDDOS Overlay Initiative

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

Overlay network is a solution for solve DDOS problem for a network users constituency, 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.

CS Danube (Cyber Security in Danube Region) project is part financed by the European Union from the START Danube Region Project Fund.

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

CS Danube (Cyber Security in Danube Region) project is part financed by the European Union from the START Danube Region Project Fund.

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

CS Danube (Cyber Security in Danube Region) project is part financed by the European Union from the START Danube Region Project Fund.

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.

CS Danube (Cyber Security in Danube Region) project is part financed by the European Union from the START Danube Region Project Fund.

Question & Answers?

CS Danube (Cyber Security in Danube Region) project is supported by START Programme within the EU strategy for Danube Region.