Denial-of-Service attack research

O.P. Voitovych
Information Security Department
Vinnytsia National Technical University, Ukraine
voytovych.op@gmail.com

E.I. Kolibabchuk
Information Security Department
Vinnytsia National Technical University, Ukraine
ekolibabchuk4@gmail.com

Дослідження атак на відмову в обслуговуванні

О. П. Войтович
кафедра захисту інформації
Вінницький національний технічний університет,
Україна
voytovych.op@gmail.com

Е.І. Колібабчук
кафедра захисту інформації
Вінницький національний технічний університет,
Україна
ekolibabchuk4@gmail.com

***Abstract* – Methods and ways to perform denial-of-service attack are analyzed and classified in this work. Famous Denial-of-Service attack classifications are reviewed and analyzed. Elements of modern DoS attack classification are proposed – classification by the amount of devices, by time, by the source computers belonging, by the source computer list, by the triggering, by the correctness of the source address, by the vulnerability, by the type, by the geographical position of sources, by power dynamics, by power layer and by effect.**

***Анотація* — У статті проаналізовано та класифіковано засоби та способи проведення атак на відмову в обслуговуванні. Розглянуто та проаналізовано відомі класифікації атак на відмову в обслуговуванні. Запропоновано нові елементи сучасної класифікації атак на відмову в обслуговуванні – класифікація за кількістю задіяних пристроїв, за часовими параметрами, за приналежністю, за наявністю списку джерел, за способом активації, за коректністю адреси-джерела, за вразливістю, за типом, за географічним положенням, за динамікою, за рівнем та за впливом.**

Keywords: denial-of-service attacks, classification, computer networks.

Ключові слова: атаки на відмову у обслуговуванні, класифікація, комп'ютерні мережі.

I. INTRODUCTION

One of the most wide-spread threats in our time for computer networks and systems is Denial-of-Service attack. The Denial-of-Service attack makes impossible system operation and partially or completely disables an access to resources and services for users. Its important to not only detect the fact of attack but also to properly identify attack type to increase effectiveness of DoS-preventing technologies.

To simplify detecting and preventing Denial-of-Service attacks a clear good-structured classification of the DoS attacks is required. Currently there are a lot of different classifications of DoS attacks, the basic is Mirkovic's classification [1] but there is still no good classification adapted for today's features and trends with a possibility to use with real systems.

II. RESEARCH OF DOS ATTACKS

The main proposed classification criterion is listed below.

By the amount of source devices – DoS attacks can be divided into simple DoS attacks, group DDoS attacks (with up to 100 devices) and massive DDoS attack (more than 100 devices).

According to attack source computers belonging to malicious attacks can be divided into voluntary attacks from intruder's machines, attacks that use bot networks, attacks that use physical and virtual dedicated servers, tunnelled attacks and random users' attacks.

Attacks from bot networks can be divided into attacks that use infected servers, infected home computers and mobile devices. It's important to know that mobile devices' IP address is not constant and can be changed every time user connects to different wireless network.

By the list of source computers DoS attacks can be divided into static-listed (fixed list of computers), controlled dynamic-listed (list of attacking sources constantly changes but there is a list of possible attack sources somewhere and dynamic unlisted when there is no way to constantly determine the list of attack sources.

By the triggering attacks can be divided into manual (when attacker manually crafts each required packed), controlled (when distributed attack is remotely controlled) and automatic (when the attack is triggered without manual actions).

Controlled attacks can be divided by the way of controlling into direct-controlled attacks (attack is controlled from the single point and infected computers has open ports that allows to identifyfy them) and indirect-controlled (attack is controlled with reverse-connections or additional protocols like BitTorrent or IRC) [2].

Direct-controlled attacks can be divided by the way that infected computers are added into network into: random scanning (attacker randomly scans IP-addresses looking for infected computers), list scanning (attacker uses the list of infected machines) and reverse-scanning (infected machines notify the attacker themselves).

Attacks can also be divided by the geographical position of sources into local (regional) and worldwide. It's useful for better recognizing legitimate traffic.

By spread in time attacks can be divided into real-time attacks which action «just now» and scheduled attacks that can change during the time of attack or be planned to change during a period of time.

By the correctness of the source address attacks can be divided into: attacks with correct source addresses (it's possible to determine the source of the attacking machine), spoofed attacks (the source address in packets is malformed) and reverse-attacks (use servers' replies for attacking, for example DNS.

By the type of the vulnerability attacks can be divided into protocol attacks and current implementation attacks.

By the power dynamics attacks can be divided into the attacks with constant power, attacks with randomly changing power, attacks with determined changing power, attacks with fluctuating power and attacks with increasing power.

By the layer attacks can be divided into attacks on physical layer (physical intrusion into a computer system, a cable break, radiation), attacks on the data link layer [3] (overloading on the frame layer), attacks on the network level (attacks on the IP protocol layer), attacks on the transport layer (attacks on the layer of datagram and segment), attacks on the session layers (attacks inside of logical connections), application level attacks [4] (attacks on the application protocols like HTTP or FTP) and attacks on services (attacks on the application that runs on top of the application layer, e.g. cloud service or web framework) [5].

By the effect attacks can be divided into blocking attacks (as a result it's impossible to connect to service for users), draining attacks (attacks drain a lot of resources but the service remains available) and damaging attacks (they damage an attacking component for example a cache, file system or protection mechanisms and as a result the data can be lost).

Blocking attacks can be divided into repairable and non-repairable. Attack is repairable when the service becomes available again after the attack stops without any manual actions.

III. EXAMPLES

The application of this proposed classification is an identification of the DoS-attack using proposed methods.

For example, Slowloris attack. By the amount of devices it's usually a single device attack or group attack because usually it's enough to use the single device to block access to webserver. By the source computer it's usually voluntary. Because of using a single computer it's a static-listed manually triggered attack. It's a semantic type of attack because it just exceeds the limit of opened connections. The source address it's correct because web server should respond to request. The vulnerability there is in the implemention, not in HTTP protocol. Only some web servers are affected, for example Apache. By power dynamics it's a constant attack. It's an application-level attack (on HTTP server) [7]. By the effect the attack is repairable blocking.

SUMMARY

There were reviewed and analysed known Denial-of-Service attack classifications in this paper.

New modern criteria of different types of Denial-of-Service attack depending on different aspects was proposed for future development.

Future plans are to complete investigation of different Denial-of-Service attacks and to improve proposed classification.

REFERENCES

[1] J. Mirkovic, A taxonomy of DDoS attack and DDoS defense mechanisms / J J Mirkovic, P Reiher // ACM SIGCOMM Computer Communication. – 2004. – Режим доступу до ресурсу : https://www.researchgate.net/profile/Peter_Reiher/publication/2879658_A_taxonomy_of_DDoS_attack_and_DDoS_defense_mechanisms/links/02e7e51d1ce0432910000000.pdf.

[2] Z. Chi. Detecting and blocking malicious traffic caused by IRC protocol based botnets / Z. Chi, Z. Zhao // Parallel Computing Workshops. – 2007. – Режим доступу до ресурсу: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4351531.

[3] S. Mansfield-Devine / Anonymous: serious threat or mere annoyance? / S. Mansfield-Devine // Network Security. – 2011. – Режим доступу до ресурсу: http://www.sciencedirect.com/science/article/pii/S1353485811700046.

[4] D. Hobbs / Using Spreadsheets as a DDoS weapon / D. Hobbs // Radware Blog – 2012. – Режим доступу до ресурсу: https://blog.radware.com/security/2012/05/spreadsheets-as-ddos-weapon/.

[5] P. Ipeirotis / The Google attack: How I attacked myself using Google Spreadsheets and I ramped up a $1000 bandwidth bill / P. Ipeirotis // A Computer Scientist in a Business School – 2012. – Режим доступу: http://www.behind-the-enemy-lines.com/2012/04/google-attack-how-i-self-attacked.html.

[6] E. Cambiaso / Slow DoS attacks: definition and categorization / E. Cambiaso, G. Papaleo, G. Chiola, M. Aiello // International Journal of Trust Management in Computing and Communications. – 2013. – Режим доступу до ресурсу: http://www.inderscienceonline.com/doi/abs/10.1504/IJTMCC.2013.056440.