УДК 004.056 : 004.424.47

Колібабчук Е. І.
Науковий керівник: к. т. н., доц. Войтович О. П.

ДОСЛІДЖЕННЯ DOS-АТАК

Вінницький національний технічний університет

Анотація: *У статті проаналізовано та класифіковано засоби та способи проведення атак на відмову в обслуговуванні.*

Ключові слова: *хакерська атака, відмова в обслуговуванні, бот-мережі.*

Abstract: *Methods and ways to perform denial-of-service attack are analyzed and classified in this work.*
Keywords: *hackers' attack, denial-of-service, bot networks.*

В сучасному світі з кожним днем збільшується використання комп'ютерів та комп'ютерних мереж. Все більш розповсюдженими є як мобільні пристрої – телефони та планшети, так і розумна побутова електроніка – телевізори, холодильники, сучасні ігрові приставки. Однією з найбільш розповсюджених загроз є атака на відмову в обслуговуванні. Ця атака унеможливлює роботу системи, частково або повністю блокує необхідні користувачу ресурси та послуги.

Атаки на відмову в обслуговуванні можна поділити на 2 великі групи – власне Denial-of-Service-атаки та Distributed-Denial-of-Service-атаки. Остання характеризується використанням декількох мережевих вузлів для реалізації атаки, зазвичай достатньо велика кількість, що значно утруднює виявлення такої атаки та захист від неї.

Для полегшення виявлення та захисту від подібних атак необхідно мати чітку класифікацію за різними критеріями. На даний момент існує велика кількість класифікацій DoS-атак, базовою з яких вражається [1], проте такої, яка б дозволила максимально охопити всі сучасні особливості проведення DoS-атак, з можливістю застосовувати в реальних системах не має.

Основні запропоновані критерії класифікації наведено нижче (рис. 1).

За кількістю задіяних пристроїв – за цією ознакою атаки можна поділити власне на: прості DoS-атаки; групові DDoS-атаки – з використанням невеликої кількості добровільно задіяних комп'ютерів (до 100 пристроїв) та масовані DDoS-атаки – більше 100 пристроїв.

Відповідно слід розрізняти методи боротьби з такими атаками. У разі простих, або групових атак достатнім може бути блокування пакетів з відповідних машин в ручному режимі за принципом чорного списку. У разі масованих атак проблематично заблокувати усі можливі джерела атаки у ручному режимі, а особливо відрізнити легальних користувачів від атакуючих.

За приналежністю джерел атаки до зловмисника атаки можна поділити на: добровільні атаки з машин зловмисників, атаки з використанням бот-мереж, атаки з використанням фізичних та віртуальних виділених серверів, атаки з використанням проміжних машин та засобів тунелювання та атаки з використанням випадкових користувачів.

Необхідно звернути увагу на те, що якщо атака виконується з виділених серверів, трафік може бути значним навіть при невеликій кількості пристроїв, оскільки подібні сервери зазвичай мають багатогігабітні канали. При забезпеченні захисту від атак з проміжних засобів тунелювання необхідно враховувати, що один засіб тунелювання може одночасно використовуватись як для атаки так і для легального доступу для сервісу, розпізнавання цієї різниці може викликати труднощі.

Атаки з використанням бот-мереж можна поділити на атаки з використанням заражених серверів [2], атаки з використанням заражених домашніх комп'ютерів та атаки з використанням заражених мобільних пристроїв.

За складом машин-джерел атаки DoS-атаки можна поділити на статичні (використовується фіксована кількість конкретних машин), динамічні з керуванням (кількість та розташування машин-джерел атаки може змінюватись з часом, при цьому існує конкретний перелік можливих джерел атаки – список IP-адрес, нод Tor або IP-адреси користувачів IRC-каналу) та динамічні без керування – відрізняються відсутністю технічної можливості встановити список машин-джерел атаки.

За засобом керування атаки можна поділити на: ручні (зловмисник вручну створює кожний необхідний пакет), керовані (розподілена атака керується віддалено) та автоматичні (атака виконується без втручання людини).

Відповідно засоби керування атакую можна розділити за засобом комунікації на пряме керування – централізоване керування з одного центра, машини мають відкритий порт, за яким можна ідентифікувати машини-джерела та непряме керування – машини не мають відкритого порта, керуються за допомогою реверс-з'єднань або додаткових протоколів (IRC, BitTorrent) [5].

Рисунок 1 – Класифікація DOS-атак

Керовані атаки з прямим керуванням можуть можна поділити за засобом включення у мережу: на випадкове сканування – зловмисник випадково сканує IP-адреси на наявність заражених машин, сканування за списком – зловмисник має список заражених машин та зворотній зв'язок – заражені машини приховано повідомляють про своє зараження.

За типом вразливості атаки можна поділити на семантичні – використання особливостей конкретного протоколу або сервісу та flood – спроби «тупого» перевантаження за допомогою величезної кількості або розміру пакетів.

За коректністю адреси джерела атаки можна поділити на: атаки з вказуванням коректного джерела – можливо чітко визначити адресу джерела атаки в пакеті даних, атаки з вказуванням підробленого джерела – адреса джерела в пакеті відсутня або вказана некоректно та реверс-атаки (amplification attack) – використання відповіді сервера для атаки (DNS, Google), відповідно складається враження, що атаку виконує легальний сервіс, який насправді просто відповідає на некоректно сформовані запити.

За динамікою потужності атаки можуть бути поділені на: атаки з постійною потужністю – атака виконується з фіксованою потужністю, атаки з випадковою змінною потужністю – потужність атаки змінюється випадковим чином, атаки з визначеною змінною потужністю – потужність змінюється за відомим алгоритмом, атаки з потужністю, що коливається – потужність атаки коливається або пульсує, атаки з потужністю, що збільшується – потужність атаки постійно збільшується.

За рівнем реалізації атаки можна поділити на атаки на фізичному рівні – фізичне втручання в комп'ютерну систему, таке як обрив кабелю, збільшення напруги, випромінювання, атаки на канальному рівні [4] – атака на рівні фізичної адресації та кадрів, атаки на мережному рівні – атака на рівні IP-пакетів, атаки на транспортному рівні – атака на рівні сегментів та дейтаграм, атаки на сеансовому рівні – атака у межах логічних з'єднань, атаки на прикладному рівні – атака з використанням протоколів прикладного рівня [3] та атаки на рівні сервісів – атака з використанням особливостей конкретного додатку або сервісу [6].

Необхідно враховувати, що чим вищий рівень атаки, тим менше сервісів вона вражає. Відповідно атака на фізичному рівні або мережному рівні може вивести з ладу всю мережу підприємства, атака на прикладному рівні – веб-сервер з усіма розміщеними сайтами, а атака на рівні сервісу лише заблокує використання конкретного сервісу, наприклад певного веб-сайту.

За впливом на жертву атаки можна поділити на атаки, що блокує доступ – результатом є блокування з'єднань сервісу з клієнтами, атаки, що збільшує споживання ресурсів – не блокує доступ повністю, а лише значно збільшує споживання ресурсів, атаки, що призводить до руйнування – наслідком атаки є руйнування компонентів системи – втрачання даних внаслідок переповнення жорсткого диску, перегрівання та вихід з ладу обладнання.

Блокуючи атаки можна поділити на атаки з можливістю відновлення – з'єднання клієнтів стане можливим, як тільки атака припиниться та атаки без можливості відновлення – з'єднання клієнтів не стане, як тільки атака припиниться – необхідне ручне втручання, можливо відновлення даних. За типом вразливості атаки можна поділити на атаки на протокол та атаки на реалізацію.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Mikrovik J. 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. Sah JJ. Impact of DDOS attacks on cloud environment / JJ Sah, DLJ Malik // IJRCCT. – 2013. – Режим доступу до ресурсу: http://ijrcct.org/index.php/ojs/article/download/276/pdf.
3. J. Yu. A detection and offense mechanism to defend against application layer DDoS attacks / J. Yu, Z. Li, H. Chen, X. Chen // Networking and Services. – 2007. – Режим доступу до ресурсу: https://www.researchgate.net/profile/Xiaoming_Chen17/publication/4314603_A_Detection_and_Offense_Mechanism_to_Defend_Against_Application_Layer_DDoS_Attacks/links/546ee4da0cf29806ec2ebfeb.pdf.
4. V. Gupta. Denial of service attacks at the MAC layer in wireless ad hoc networks / V. Gupta, S. Krishnamurthy // MILCOM. – 2002. – Режим доступу: https://www.cs.wmich.edu/wise/doc/spins/dos/denial-of-service-attacks.pdf.
5. 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.
6. M. Srivatsa / Mitigating application-level denial of service attacks on Web servers: A client-transparent approach / M. Srivatsa, A. Iyengar, J. Yin, L. Liu // ACM Transactions on the Web. – 2008. – Режим доступу до ресурсу: http://researcher.ibm.com/files/us-aruni/TWEBDos.pdf

Колібабчук Едуард Ігорович факультет інформаційних технологій так комп'ютерної інженерії, студент групи БС-12б, Вінницький національний технічний університет, Вінниця, alien@openmailbox.org.

Войтович Олеся Петрівна кандидат технічних наук, доцент кафедри захисту інформації, Вінницький національний технічний університет, Вінниця.

Kolibabchuk Eduard faculty of Information Technologies and Computer Engineering, student group BS-12b, Vinnytsya National Technical University, Vinnytsya, alien@openmailbox.org.

Voitovych Olesya Petrivna, Ph.D. docent, docent of Vinnytsia National Technical University, Vinnytsia, Faculty for Information Technologies and Computer Engineering, chair of information security.