***Куля Ю.Е.**, кандидат технічних наук, доцент,*
Квашенко В.Р.

АНАЛІЗ DDOS АТАК НА ПІДПРИЄМСТВА ТА МЕТОДИ ЇХ ПРОТИДІЇ

За останні роки середовище інформаційної безпеки зазнало великих змін. З одного боку, з розвитком технологій і прогресом мережевої інтеграції мережі набувають все більшого масштабу, а їх структура стає все більш складною. З іншого боку, розвиваються технології проведення атак на ці мережі. Методи грубої сили та масштаб ботнетів більше не є основними факторами, що визначають успішність атаки. Навпаки, зловмисники з більшою ймовірністю вдадуться до інформаційних комплексних комбінованих атак із чіткими цілями атаки. Ці зміни створили серйозні проблеми для захисту мережі. Таким чином, з точки зору використання захищеного мережного середовища, ця стаття вивчає випадки проведених атак на відомі компанії, типи атак та методи захисту від них. (Ankit & Vishwakarma, б. д.)

Зважаючи на те, що простої IT-послуг коштують великим компаніям від 300 000 до понад 1 000 000 доларів США на годину, можна зрозуміти, що фінансовий удар від навіть короткої DDoS-атаки може серйозно зашкодити вашому прибутку. 16 жовтня 2020 року група аналізу загроз (TAG) Google зафіксувала рекордну атаку UDP Amplification, яка залишається найбільшою атакою на компанію, тривала шість місяців і досягала 2,5 Тбіт/с (Huntley, 2020).

Відмова в обслуговуванні (DoS) атак на мережі є численними і потенційно руйнівним. На даний момент ідентифіковано багато типів DoS-атак, і більшість із них досить ефективні для припинення обміну даними в мережах. Ці напади стосуються будь-якого використання одного комп'ютера або кількох комп'ютерів, які називаються зомбі.

UDP Amplification, або розподілена рефлексивна відмова в обслуговуванні (DRDoS) це — форма розподіленої атаки на відмову в обслуговуванні (DDoS), яка покладається на загальнодоступні сервери UDP і коефіцієнти посилення пропускної здатності (BAF), щоб перевантажити систему жертви трафіком UDP. За задумом UDP — це протокол без підключення, який не перевіряє адреси джерела Інтернет-протоколу (IP). Якщо протокол прикладного рівня не використовує контрзаходи, такі як ініціювання сеансу в протоколі передачі голосу через Інтернет, зловмисник може легко підробити дейтаграму IP-пакету (основну одиницю передачі, пов’язану з мережею з комутацією пакетів), щоб включити довільну IP-адресу джерела. Коли IP-адреса джерела багатьох UDP-пакетів підроблена до IP-адреси жертви, сервер призначення (або підсилювач) відповідає жертві (замість зловмисника), створюючи відображену атаку відмови в обслуговуванні (DoS).Зловмисники можуть використовувати пропускну здатність і відносну довіру великих серверів, які надають

протоколи UDP, надані в цьому сповіщенні, щоб наповнювати жертв небажаним трафіком і створювати DDoS-атаку.

Виявлення атак DRDoS непросте через використання великих надійних серверів, які надають послуги UDP. Оператори мереж, які надають ці послуги, які можна використовувати, можуть застосовувати традиційні методи пом'якшення DoS. Щоб виявити атаку DRDoS, стежте за надто великими відповідями на певну IP-адресу, що може вказувати на те, що зловмисник використовує службу.

Для захисту від UDP Amplification атак можна використовувати мережевий потік для виявлення підроблених пакетів. Також можна використовувати аналізатори трафіку або інші узагальнені дані про інтернет трафік для моніторингу незвичайної кількості запитів до служб UDP. Або ж використовувати індикатори мережного трафіку для виявлення аномалій обслуговування, аномалії байтів на пакет або пакетів за секунду.

AWS повідомила про пом'якшення масштабної DDoS-атаки в лютому 2020 року. На піку цієї атаки вхідний трафік передавався зі швидкістю 2,3 Тбіт/с. AWS не розголошує, який клієнт став ціллю атаки. Зловмисники використовували зламані веб-сервери CLDAP. CLDAP — це протокол для каталогів користувачів. Це альтернатива LDAP, старішій версії протоколу. Протягом останніх років CLDAP використовувався в багатьох DDoS-атаках. (Famous DDoS attacks | The largest DDoS attacks of all time, б. д.)

Для захисту від цих атак, підприємства можуть запроваджувати інструменти та послуги пом'якшення DDoS-атак. Підприємства також можуть впровадити захисні міри лише в тих системах, які можуть бути використані зловмисниками для атак, як-от DNS або NTP, за допомогою брандмауера від Інтернету. Інтернет-сервіси також можна захистити шляхом обмеження швидкості або іншого методу захисту вихідних повідомлень. Пом'якшення цієї атаки відображення починається з розуміння протоколу CLDAP, а також відповіді на запитання, навіщо підприємству сервер CLDAP або LDAP, який використовується для призначення IP-адрес хостам у локальній мережі, доступним безпосередньо з Інтернету.

Найефективнішим засобом пом'якшення може бути блокування доступу до серверів LDAP з Інтернету. Найкращий підхід — заборонити LDAP через Інтернет за допомогою правил брандмауера; або заборонити весь трафік на порту 389, або обмежити доступ до певних IP-адрес або Mac-адрес. Це не завжди можливо, оскільки основні віддалені служби можуть покладатися на LDAP (або Active Directory). Вимкніть просте прив'язування LDAP і Unsigned Simple Authentication and Security Layer (SASL) у конфігурації, так як ці два потоколи є вразливі до даного типу атаки. На заміну ним використовуйте «Захищений LDAP» (LDAPS), який вимагає автентифікації та авторизації для обмеження доступу. Захищений LDAP працює на порту 636.

У цій статті було розглянуто механізми проведення DDoS атак на підприємства. Для цього було проаналізовано найчастіші використовувані типи DDoS атак, ними виявились UDP

Amplification та CLDAP Reflection Attack. Було проаналізовані методики проведення цих атак та наведено рекомендації як захиститись від них.

В майбутньому механізми атаки будуть еволюціонувати, знаходити нові методики та способи проведення атак, що стане приводом для покращення механізмів захисту від цих атак.

Список використаних джерел:

Ankit, J., & Vishwakarma, R. (б. д.). A survey of DDoS attacking techniques and defence mechanisms in the IoT network - Telecommunication Systems. SpringerLink. https://link.springer.com/article/10.1007/s11235-019-00599-z

Huntley, S. (2020, 16 жовтня). How we're tackling evolving online threats. Google. https://blog.google/threat-analysis-group/how-were-tackling-evolving-online-threats/

Famous DDoS attacks | The largest DDoS attacks of all time. (б. д.). Cloudflare. https://www.cloudflare.com/learning/ddos/famous-ddos-attacks/