*Інформаційні технології*

**Борисенко Богдан Володимирович**

аспірант кафедри інформаційних управляючих систем і технологій, факультету інформаційних технологій, Ужгородського національного університету, м. Ужгород, Україна, https://orcid.org/0000-0003-1320-5083

**Оцінка характеру ураження комп'ютерних систем в залежності від сфери їх застосування**

З розвитком технологій кількість людей, які використовують комп’ютери, сьогодні зростає. Таке збільшення використання комп’ютерів спричиняє збільшення різноманітності атак і кількості атак на комп’ютерні системи. Ця ситуація розкриває важливість захисту даних, що обробляються на комп'ютерах, і концепції інформаційної безпеки. Завдяки системам виявлення вторгнень, які займають важливе місце в захисті комп’ютерних систем, атаки на комп’ютери та комп’ютерні мережі можна виявити до того, як вони вплинуть на системи. Враховуючи зростання різноманітності атак, розробка систем виявлення атак стала предметом багатьох досліджень останнім часом. Загалом категорії комп'ютерних систем в залежності від сфери їх застосування, які стали жертвами атак у 2022 році відсотково розподіляються наступним чином (рисунок 1) [1].

**Рис.1. Категорії комп'ютерних систем в залежності від сфери їх застосування, які стали жертвами атак у 2022 році**

Жертвами атак ставали насамперед приватні особи та держустанови, а атаки найчастіше були спрямовані на отримання конфіденційної інформації. В даний час мережеві атаки класифікуються за деякими параметрами, а саме за характером впливу на мережу, за метою атаки, за наявністю зворотного зв'язку з мережею, що атакується, за умовою початку атаки, за розташуванням суб'єкта по відношенню до обсягу атаки і за рівнем еталонної моделі ISO/ OSI. У свою чергу, з наведеної вище класифікації атаки поділяють на: DoS-атаки, DDoS, фішинг, ARP-спуфінг, MAC-флуд-атака, DNS-кеша, IP Spoofing, ACK-флуд, Brute-force, перехоплення TCP-сеансу, атака «Man-In-The-Middle», IDOR-уразливість, сканування портів, ICMP-тунелювання, LOKI атак, XSS-уразливість, SQL-ін'єкції.

Фахівці виділяють шість видів найпопулярніших атак: Фішинг; DDoS; Brute-force; IDOR-уразливість; XSS-уразливість; SQL-ін'єкція. Фішинг займає особливу увагу серед інших способів отримання несанкціонованого доступу до даних. Шахраї створюють копії начебто звичайних або популярних сайтів і збирають номери банківських карток, паролі до електронної пошти та інших сервісів, а також інформацію про облікові записи. У методиці «фітингу» використовують різні способи крадіжки особистої інформації.

DDoS (розподілена відмова в обслуговуванні) – це спроба вивести сервер з ладу. Для цього хакер підключає заражений вірусом комп'ютер або його IoT-пристрій до мережі ботнета, імітуючи потік запитів на сервер, який він не може обробити. Користувачі просто не можуть отримати доступ до сайту, тому що сервер відсортував чергу фіктивних запитів [2].

Brute-force дозволяє шкідливій програмі отримати доступ до системи або її окремих захищених областей, відправляючи на сервер різні комбінації символів, сподіваючись отримати однакову пару «логін-пароль». У вразливості IDOR (небезпечне пряме посилання на об'єкт) у ролі незахищених об'єктів найчастіше виступають URL-адреси сторінок, файлів та каталогів, доступні всім користувачам.

XSS-вразливість (міжсайтовий скриптинг) – атака, що використовує вразливості для впровадження тегів HTML або коду JavaScript на сторінки веб-сайту. Часто використовується в динамічних сайтах і виникає коли розробник не відфільтрував дані, які користувач ввів на сайт. Таким чином, зловмисник може, наприклад, просто вставити скрипт у вікно повідомлення на форумі і опублікувати його, і як тільки користувач відкриє цю сторінку, скрипт буде виконаний і почнеться атака.

В результаті хакери можуть змінювати сторінки сайту, впроваджувати скрипти у код для збільшення кількості переглядів на інших сайтах або добувати криптовалюту. Це може бути причиною того, що комп'ютер останнім часом працює повільно.

Захист XSS – це знешкодження шкідливого JS-коду. SQL-ін'єкція, аналогічно, тобто за допомогою введення користувача на сторінці, дає можливість зловмиснику змінити свої запити GET або POST і файли cookie для доступу до бази даних, особливо якщо у неї архітектура MySQL.

Сучасне суспільство та організації можуть захищати свої передані дані різними способами, як із застосуванням спеціальних програм, так і просто дотримуючись ряду правил. Такими правилами є створення складних паролів у яких не згадується день народження, місце роботи та інші дані власника сторінки або адміністратора системи, за якими цей пароль можна підібрати, відключення функції автозаповнення полів для логіну та пароля, уникнення загальнодоступних WiFi-мереж, двофакторна автентифікація, очищення cookies та використання надійного антивіруса. Доцільно своєчасно проводити оновлення програмного забезпечення, адже розробники невпинно працюють над удосконаленням додатків, включаючи пункт безпеки даних.

**Література**:

1. InterFax-Україна. Інформаційне агентство. Режим доступу – <https://interfax.com.ua/news/interview/911979.html>
2. Kulwanth Bandi, Srinivasarengan V., Anish Peddinte, Abirami K. Detect and Alleviate DDoS Attacks in Cloud Environment. 2024. DOI: 10.1007/978-981-99-7633-1\_17.