УДК 004

ОСНОВНІ ВИДИ КІБЕРАТАК ТА ОПЕРАЦІЙ У КІБЕРВІЙНІ В УКРАЇНІ

MAIN TYPES OF CYBER ATTACKS AND OPERATIONS IN THE CYBER WAR IN UKRAINE

Олександр Капись

Державна служба спеціального зв'язку та захисту інформації України

Російська загарбницька війна проти України демонструє важливу динаміку щодо кібер загроз, нових векторів атак та використання вразливостей. Кібератаки та операції були розгорнуті з метою знищити дані та системи, порушити роботу критичної інфраструктуру та служб, взяти під контроль інформаційний простір, отримувати доступ до великих обсягів даних, вести розвідку та шпигунство та здійснювати операції впливу. На основі даних якими володіє CERT-UA (Урядова команда реагування на комп'ютерні надзвичайні події) було проаналізовано та виділено наступні типу кібероперацій які використовуються у війні проти України.

Деструктивні атаки – кібератаки, спрямовані на остаточне видалення даних або пошкодження систем, що робить їх неможливими для відновлення. Ці атаки можуть мати довгострокові наслідки для організацій, якщо в організаціях не задіяні методи резервування даних та сервісів. Найпопулярнішими прикладами шкідливого програмного забезпечення, яке використовується для здійснення деструктивних атак були WhisperGate / WhisperKill, FoxBlade, HermeticRansom, CaddyWiper, DesertBlade, Industroyer2, Lasainraw, FiberLake. Головними гравцями які використовують даний тип атак проти України являються представники головного управління розвідки росії, а саме угрупування Sandworm та APT28.

Підривні атаки – кібератаки, спрямовані на порушення роботи сервісів та операцій, які активно використовуються під час війни, в тому числі проти українських організації на ранніх стадіях вторгнення. Розподілені атаки на відмову в обслуговуванні (DDoS) були найпоширенішими типами атак, що спостерігалися під час цієї війни, що впливають на державний та фінансовий сектори. На DDoS-атаки припадає 87,5 % усіх кібератак. Найбільше постраждали фінансовий, державний та ІКТ-сектори. Особливо шкідливою тенденцією є націленість на українські неприбуткові організації, які є вразливою мішенню через їхню загальну низьку готовність та відсутність заходів стійкості від даного типу атак.

Використання персональних даних у вигляді зброї – кібератаки, що призводять до крадіжки чи витоку даних або отримання даних з метою шпигунства, спостереження чи розвідки. Головним методом отримання доступу до персональних даних це використання найслабшої ланки в будь якій організації в плані забезпечення належного рівня кібербезпеки, а саме людини. Найбільш поширеним методом розповсюдження шкідливого програмного забезпечення за допомогою якого можливо отримати доступ до критичної інформації являється фішинг. Цим типом кібероперацій займаються представники фсб росії, а саме угрупування Gamaredon, EnergeticBear та Turla.

Дезінформація – атаки пов'язані з поширення неправдивої інформації та пропаганди. Суб'єкти загрози мають на меті вплинути на інформаційний простір та обмежити доступ населення до своєчасної, достовірної та офіційної інформації, або цілеспрямовано ввести в оману та підірвати інформацію.

Таким чином, розуміючи головні типи кібероперацій, методи та методики їх реалізації що застосовуються в кібервійні проти України можливо мінімізувати можливі наслідки та підвищити ефективність вже існуючих систем забезпечення кібербезпеки як для державних організацій, так і для представників комерційних організацій.

Бібліографія

1. CERT-UA. URL: https://cert.gov.ua/
2. An overview of Russia's cyberattack activity in Ukraine. URL: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd
3. Defending Ukraine: Early Lessons from the Cyber War. URL: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK
4. The role of cyber in the Russian war against Ukraine: Its impact and the consequences for the future of armed conflict.URL:https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/702594/EXPO_BRI(2023)702594_EN.pdf