УДК 004.056.5:004.942

ВИКОРИСТАННЯ СЛАБКИХ ЛАНЦЮЖКІВ МЕРЕЖЕВИХ ІГОР ЯК ТОЧКИ ВХОДУ В КОРПОРАТИВНІ МЕРЕЖІ

[1]Полотай О.І., [2]Дітковський М.М., [1]Гуменюк М.Р.
[1]Львівський державний університет безпеки життєдіяльності
[2]Національний університет Львівська політехніка

Анотація. *Розглядається малодосліджений вектор кіберзагроз — використання слабких елементів мережевих ігор як потенційних точок проникнення у корпоративні мережі. Окреслено типові сценарії атак, способи маскування шкідливої активності під ігровий трафік, а також наведено рекомендації щодо мінімізації ризиків і підвищення кіберстійкості.*

Ключові слова : *мережеві ігри; кіберзагрози; корпоративна мережа; уразливості; P2P-з'єднання; ігрові модифікації; шкідливе програмне забезпечення; соціальна інженерія; інформаційна безпека; кіберстійкість; вектори атак; контроль програмного середовища.*

Сучасні корпоративні мережі дедалі частіше зазнають атак не через класичні вектори проникнення, а через малопомітні побічні канали, пов'язані з цифровою поведінкою працівників. Однією з таких недооцінених загроз є використання мережевих ігор, які встановлюються на робочих станціях або запускаються через браузер. Оскільки більшість компаній не розглядають геймінг як серйозний фактор кіберризику, ігрові клієнти, сторонні лаунчери та внутрішньоігрові сервіси часто залишаються поза увагою систем технічного захисту інформації. Це створює можливість для атакувальників використовувати слабкі компоненти ігор як точку входу в корпоративне середовище.

Мережеві ігри використовують складну інфраструктуру: центральні сервери, peer-to-peer-механізми, голосові чати, моди, плагіни та сторонні лаунчери. Більшість із цих компонентів не проходять комплексної перевірки безпеки на рівні корпоративного ІТ. На відміну від бізнес-ПЗ, ігрові програми часто мають нерегулярні оновлення, невідомі залежності, слабко захищені протоколи передачі даних та високий рівень довіри з боку користувача, що відкриває можливості для інжекції шкідливого коду.

В таблиці 1 показано найбільш популярні онлайн-ігри.

Таблиця 1 – Сучасні онлайн-ігри

Назва гри	Платформи	Особливості
World of Tanks	ПК, консолі, мобільні	Класика MMO-танків
World of Tanks Blitz / Modern	Мобільні / консолі	Мобільні/консольні версії WoT

Armor		
World of Tanks: Heat	ПК, консолі (PS5, XSX/S), Steam Deck	Hero-shooter у танковому сеттингу
War Thunder	ПК, консолі	Реалістичний симулятор
Armored Warfare	ПК	Сучасні танки + PvE
Enlisted	ПК	Історичні кампанії WWII
Call of War: WWII	Браузер	Глобальна стратегія/MMO
Diep.io	Браузер / мобільні	Легка .io-гра
BZFlag	ПК	Open-source 3D FPS-танки
Tanki Online	Браузер	Кастомізація, PvP, івенти
Modern Tanks (Steam)	ПК (Steam)	Аркадний топ-down танковий шутер

В сучасних комп'ютерних топологіях існують такі типові місця потенційного проникнення в корпоративну мережу через мережеві ігри:

1. P2P-з'єднання між гравцями, які можуть бути використані для сканування відкритих портів або впровадження експлойтів на робочі станції.
2. Ігрові моди й плагіни, що часто розробляються сторонніми програмістами без аудитів безпеки; поширення модів може стати інструментом масового зараження.
3. Голосові чати та VoIP-інтеграції, уразливі до атак типу buffer overflow або компрометації протоколів передавання голосу.
4. Фішингові внутрішньоігрові повідомлення, що імітують офіційні нотифікації від ігрових сервісів, стимулюючи працівника переходити за шкідливими посиланнями.
5. Сторонні лаунчери, які збирають телеметрію, мають привілейований доступ до файлової системи та оновлюються через незашифровані канали.
6. Потрапивши на робочу станцію, шкідливе ПЗ може використати ігровий процес як маскування для аномального трафіку або lateral movement усередині мережі.

Для мінімізації таких загроз необхідно дотримуватися таких рекомендацій:

1. Заборонити запуск ігор на робочих станціях або ізолювати їх у віртуальних контейнерах.
2. Застосовувати контроль додатків з чітким переліком дозволених програм.
3. Використовувати мережеву сегментацію, щоб робочі місця з низьким рівнем довіри не мали прямого доступу до внутрішніх сервісів.
4. Активувати поведінковий моніторинг трафіку, що дозволить виявляти аномальні P2P-з'єднання.

5. Проводити корпоративні тренінги, де працівників навчають ризикам встановлення модів та сторонніх патчів.

6. Аналізувати журнали дій на робочих станціях через системи SIEM для виявлення специфічних патернів, типових для ігрового ПЗ.

Висновки. Мережеві ігри становлять малопомітний, але потенційно високоризиковий вектор проникнення в корпоративні мережі. Незахищені компоненти ігрової інфраструктури, багатокомпонентні лаунчери, моди та P2P-механізми можуть стати "слабкими ланцюжками", через які зловмисники отримують доступ до внутрішніх систем підприємства. Поєднання технічних уразливостей і ризикованої поведінки користувачів створює сприятливе середовище для проведення атак нового типу. Усвідомлення цієї проблеми та впровадження комплексних заходів контролю дозволить суттєво підвищити рівень кіберстійкості корпоративної інфраструктури та мінімізувати ризики, пов'язані з використанням розважального ПЗ у робочому середовищі

Література

1. Поширені загрози для геймерів: як суперники можуть впливати на хід гри. URL: https://www.eset.com/ua/about/newsroom/blog/home-security/osnovnyye-ugrozy-dlya-geymerov-kak-protivniki-mogut-vliyat-na-khod-igry/?srsltid=AfmBOoqmU3ieMyMCr7agDWUVKzO0Y7Z033LeULHz-5bTZgTok0_hqjz0

2. Полотай О.І., Брич Т.Б., Ткаченко А.М., Дітковський М.М., Гуменюк М.Р. Інформаційні загрози та методи забезпечення безпеки в сучасних мережевих іграх. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка». 2025. Том 2 № 30: С. 50-64.

3. 10 порад щодо безпеки в іграх онлайн. URL: https://lemon.school/blog/10-porad-shhodo-bezpeky-v-igrah-onlajn