УДК 004.056

Чабаненко К.С., Бобок І.І., Кушніренко Н.І.

Національний університет «Одеська політехніка»

МОДЕЛЬ CYBERCRIME-AS-A-SERVICE В СУЧАСНОМУ ЛАНДШАФТІ КІБЕРЗАГРОЗ

Вступ. Кіберзлочинність як послуга (Cybercrime-as-a-Service, CaaS) є однією з найбільш актуальних загроз, що докорінно трансформувала ландшафт кібербезпеки. Ця модель комерціалізувала злочинну діяльність, знизивши технічний поріг входу для зловмисників і зробивши атаки масштабованими та менш витратними. Розвиток тіньових маркетплейсів і спеціалізація акторів (наприклад, брокерів початкового доступу, розробників MaaS) призвели до формування розподіленої, професійної та стійкої злочинної екосистеми, в якій окремі компоненти кібератаки можна придбати або орендувати як послугу. У контексті гібридних конфліктів CaaS стає інструментом для досягнення не лише фінансових, але й геополітичних та руйнівних цілей.

Мета: Аналіз концепції CaaS як сучасної моделі організації кіберзлочинності, виявлення її структурних елементів, економічних та технологічних чинників розвитку, а також оцінка ризиків, які вона створює для системи кібербезпеки держави та бізнесу.

Основна частина

Ринок CaaS дуже динамічно зростає, пропонуючи клієнтам все більше різноманітних послуг. Його особливістю є запровадження в традиційний вектор атаки від розробника до жертви третю сторону: клієнта, який за плату отримує готові експлойт-набори та інструменти для виконання атак, не пишучи коду й не шукаючи вразливостей самостійно, а також орієнтація на «сервісність»: постачальники часто забезпечують цілодобову технічну підтримку, форуми для спілкування й детальні покрокові інструкції, що робить виконання атак доступнішим. Послуги можуть надаватися за різними моделями: фіксована щомісячна підписка, одноразова ліцензійна плата, відсоток від прибутку клієнтів або комбінування цих підходів. Основними моделями екосистеми CaaS є Malware-as-a-service (MaaS), Phishing-as-a-service (PaaS/PhaaS) та DDoS-as-a-service (DaaS).

Оператори MaaS пропонують широкий спектр різних типів шкідливого програмного забезпечення, найпоширенішими прикладами є: інформаційні викрадачі, завантажувачі, бекдори, шпигуньське програмне забезпечення, кейлогери, трояни і тд. Окремою, спеціалізованою реалізацією моделі MaaS є Ransomware-as-a-Service (RaaS): окрім самого шифрувальника вона зазвичай пропонує повну інфраструктуру для атаки - панель керування, канали переговорів і механізми прийому викупу - і заробляє в основному за рахунок частки від сплачених жертвами викупів.

Прикладом відомого постачальника послуг RaaS є угруповання LockBit, яке має прихований вебпортал у мережі Tor. Після реєстрації афілійовані користувачі отримували доступ до панелі керування, де могли переглядати список жертв,

статус шифрування систем, а також публікувати викрадені дані у разі відмови від сплати викупу - така тактика відома як «подвійне вимагання» (double extortion).

Сервіси PaaS надають клієнтам можливість придбання готових фішингових комплектів (phishing kits). Наприклад, популярна PaaS платформа LabHost надавала такі комплекти, що могли містити готові рішення для перехоплення 2FA-кодів через проксування трафіку (Adversary-in-the-Middle), велику бібліотеку фішингових шаблонів, можливість замовити індивідуальні фішингові сторінки під бренд-ціль, автоматичну розгортку на VPS та аналітику.

Модель, що дозволяє клієнтам оплачувати проведення DDoS-атак проти визначених цілей має назву DDoS-as-a-Service (DaaS), або також можна зустріти під назвою «DDoS-for-hire-services» та «Botnets-for-hire-services». Сервіси для проведення атак на відмову в обслуговуванні поділяються на легітимні «stressers» (для тестування власної IT-інфраструктури) та нелегітимні «booters», але, попри декларовану законність, деякі «stressers» не перевіряють право власності на цільовий сервер, що дозволяє їх використання у злочинних цілях. Типовий набір для побудови ботнету включає шкідливий модуль (payload) та інструменти для розгортання та адміністрування C2 (Command-and-Control) інфраструктури.

Для всього світу поширення ринку CaaS призводить до зростання кіберзагроз. Наразі найнебезпечнішими є DDoS, програми-вимагачі та фішинг, зокрема як вектор початкового проникнення для інших типів атак (рисунок 1).

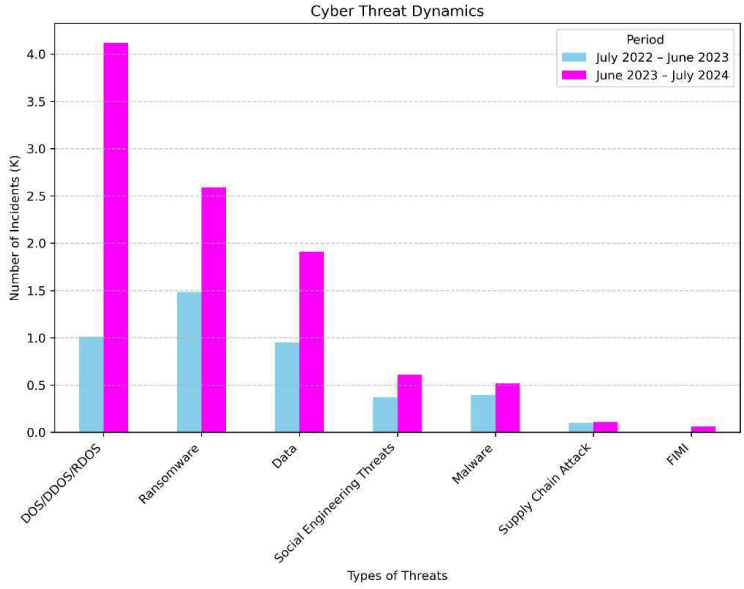

Рисунок 1 - Динаміка зростання кіберзагроз за даними звітів ENISA [1, 2]

Паралельно із розвитком CaaS зросла «площа ураження»: сучасні мобільні пристрої, гаджети та численні IoT/OT-пристрої часто мають слабкий або відсутній базовий захист, що робить їх привабливою мішенню для зловмисників і сприяє швидкому розширенню ботнетів, які використовуються у DDoS-атаках. Ботнет-сервіси часто використовуються хактивістами. Прикладом є платформа DDoSia, пов'язана з групою NoName057, яка, за даними ENISA за 2025 рік, відповідальна за понад 60 % зареєстрованих DDoS-інцидентів у Європі [3]. Також цей приклад пов'язаний із тенденцією переходу від мотивів грошової вигоди до більш складних, зокрема політичних, адже активність групи зростала в періоди, коли ЄС демонстрував підтримку окремих геополітичних ініціатив або під час

національних виборів. Зокрема, однією з причин є підтримка України.

Паралельно програми-вимагачі залишаються одним із найбільш небезпечних інструментів кіберзлочинності, попри певне коливання активності в окремі періоди. Посередники початкового доступу (Initial Access Brokers) продовжують торгувати дешевими VPN- та RDP-доступами, що спрощує проникнення в корпоративні мережі. Загалом фішинг залишається провідним вектором вторгнення - на нього припадає близько 60 % інцидентів, тоді як ще близько 21 % атак починаються з експлуатації відомих вразливостей і завершуються інфікуванням шкідливим ПЗ.

Для України розвиток CaaS має подвійний ефект. З одного боку, держава залишається ціллю численних кібератак у межах російсько-українського протистояння і не тільки, з іншого - досягає помітних результатів у протидії кіберзлочинності. Наприклад, у 2024 році українські правоохоронці спільно з міжнародними партнерами взяли участь у ліквідації угруповання LockBit та проведенні операції Endgame, що знищила інфраструктуру кількох транснаціональних кібергруп [4].

Висновки. Модель Cybercrime-as-a-Service стала однією з найвагоміших трансформацій у розвитку сучасного кіберпростору, докорінно змінивши структуру та механізми функціонування глобальної кіберзлочинності. Її поширення призвело до суттєвого зростання частоти та масштабності кіберінцидентів, серед яких домінують DDoS-атаки, кампанії програм-вимагачів і фішингові операції. Найбільш уразливими до таких загроз залишаються державний сектор і критична інфраструктура, зокрема об'єкти енергетики, телекомунікацій, промислового виробництва та фінансової сфери. Ефективна протидія CaaS вимагає комплексного, багаторівневого підходу, що поєднує розвиток систем моніторингу даркнет-ресурсів, підготовку кваліфікованих фахівців, підвищення рівня кіберобізнаності користувачів і впровадження сучасних архітектур безпеки, орієнтованих на принципи Zero Trust та Secure-by-Design.

Перелік використаних джерел

1. European Union Agency for Cybersecurity (ENISA). ENISA Threat Landscape 2023: ETL. ENISA, 2023. 160 p. [Електроний ресурс] - Режим доступу: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

2. European Union Agency for Cybersecurity (ENISA). ENISA Threat Landscape 2024: ETL. ENISA, 2024. 130 p. [Електроний ресурс] - Режим доступу: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

3. European Union Agency for Cybersecurity (ENISA). ENISA Threat Landscape 2025: ETL. ENISA, 2025. 86 p. [Електроний ресурс] - Режим доступу: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025

4. Рада національної безпеки і оборони України. Річний аналітичний огляд (жовтень 2023 – вересень 2024 рр.). – Київ: Аппарат РНБО України, 2024. 32 с. [Електроний ресурс] - Режим доступу: https://www.rnbo.gov.ua