НАТО попереджає про зростання кіберзагроз, що спрямовані проти портів

В новому звіті НАТО проаналізували кібербезпеку світових портів та відзначили зростання атак на інфраструктуру з боку російських, іранських та китайських хакерів.
Про це стало відомо зі звіту Центру передового досвіду з питань кіберзахисту НАТО (CCDCOE), пише Splash.
У документі зазначається, що порти стикаються з величезною кількістю кібератак з боку хакерів, яких підтримують РФ, Іран та Китай. Зокрема, російська APT28, пов’язана з ГРУ, іранські угруповання, такі як APT35 і MuddyWater, а також китайські операції, такі як Mustang Panda, активно атакують портові системи, включаючи системи контролю доступу, судноплавні служби та інфраструктуру паливних терміналів.
Також порти є цілями хакерів, що не пов’язані з вищезгаданими країнами. Зокрема, згадуються атаки від хакерських груп BlackCat та NoName057, які проводять DDoS-кампанії та атаки програмами-вимагачами на європейські порти в Гамбурзі та Антверпені.
В CCDCOE нагадують, що більшість світових портів перебувають у приватній власності, але виконують військові функції, проте майже не інтегровані в кіберзахист НАТО.
Тому експерти закликають до термінових реформ – оновлення морської стратегії НАТО, посилення обміну розвідданими та включення кібернавчання до навчань НАТО. Це потрібно, щоб запобігти майбутнім цифровим блокадам у світових портах.
Раніше USM повідомляв, що курсанти ВМС ЗСУ пройшли тренінг з кібербезпеки в межах програми НАТО.
https://usm.media/nato-poperedzha%d1%94-pro-zrostannya-kiberzagroz-shho-spryamovani-proti-portiv/