КВАРТАЛЬНЕ
АНАЛІТИЧНЕ

РЕЗЮМЕ

ДРУГИЙ КВАРТАЛ, 2024

Глобальні тренди

У другому кварталі 2024 року відбулося різке зростання активності китайських хакерів, що привернуло підвищену увагу урядів західних країн. У травні національна розвідка США опублікувала звіт, у якому зазначається, що Китай залишається найбільшою кіберзагрозою для Сполучених Штатів, зокрема в контексті виборів, де китайські хакери використовують штучний інтелект для розпалювання соціальної напруги.

Агентство з кібербезпеки та захисту інфраструктури США (CISA) виявило, що китайські кіберзлочинці зосередилися на атаках на критичну інфраструктуру, зокрема в авіаційному та енергетичному секторах. Основними цілями стали малі та середні підприємства, які надають важливі послуги. Федеральні чиновники також визнали, що китайська кампанія Volt Typhoon остаточно змінила ландшафт кіберзагроз. Volt Typhoon, метою якої є дестабілізація та створення суспільної паніки, особливо під час конфліктів, демонструє перехід від традиційного шпигунства до більш зловісних намірів Пекіна. Зміни підходів супроводжуються техніками, які можуть бути використані іншими іноземними супротивниками США.

Китайська кіберактивність не обмежується виключно Сполученими Штатами. Останнім часом все частіше з'являються повідомлення про кампанії кібершпигунства проти членів Міжпарламентського альянсу щодо Китаю. Зокрема, китайські хакери здійснили атаку на Голову парламентського комітету закордонних справ Бельгії. Нідерланди також виявили масштабну шпигунську кампанію китайських хакерів, які провели складну операцію з проникнення у військові мережі країни. У червні військова розвідка Нідерландів повідомила, що розслідування інциденту триває і масштаби втручання виявилися значно більшими, ніж спочатку передбачалося.

Тим часом Китай продовжує зміцнювати свої кіберсили, створивши у квітні Сили інформаційної підтримки. Попри зростання загрози з боку Китаю, експерти відзначають, що кількість пристроїв китайського виробництва у мережах США за останній рік зросла на 40%, досягнувши 300 000 пристроїв порівняно з 185 000 у попередньому році.

У другому кварталі 2024 року чітко простежується тенденція активізації діяльності правоохоронних органів у боротьбі з групами-вимагачами та їх інфраструктурою. У квітні британська поліція зупинила діяльність

Ця публікація стала можливою завдяки підтримці, наданій Агентством США з міжнародного розвитку, згідно з умовами гранту Української фундації безпекових студій в рамках Проєкту USAID "Кібербезпека критично важливої інфраструктури України". Думки автора, висловлені в цій публікації, не обов'язково відображають погляди Агентства США з міжнародного розвитку або Уряду США.

LabHost, яка надавала злочинцям послуги Phishing-as-a-Service, що використовувалися для створення початкових точок вторгнення в мережі жертв.

У травні відбулася ціла серія масштабних заходів правоохоронців. Правоохоронні органи 13 країн провели спецоперацію Endgame, яка дозволила знищити кримінальну інфраструктуру ряду зловмисних груп, зокрема IcedID, SystemBC, Pikabot, Smokeloader, Bumblebee і Trickbot. Українські правоохоронці взяли активну участь у цій операції, здійснивши більшість арештів та обшуків.

Інша операція була проведена британськими, американськими та австралійськими правоохоронцями з метою розкриття особи лідера кіберзлочинної групи LockBit, яким виявився росіянин Дмитро Хорошев. Держдепартамент США вже оголосив винагороду у розмірі 10 мільйонів доларів за інформацію, яка дозволить його затримати. Також у травні Служба безпеки України та ФБР спільно з правоохоронними органами Великої Британії та ЄС провели спецоперацію у восьми країнах Європи, викривши понад 30 учасників транснаціональних хакерських угруповань.

Проте, наразі важко сказати, чи матимуть ці заходи довгостроковий ефект. Вже у травні експерти Trellix виявили, що інфраструктура, яка належала угрупованню LockBit, активно відновлюється і знову починає функціонувати.

Розвиток штучного інтелекту (ШІ) та його вплив на сферу кібербезпеки стають все більш актуальними темами для кібербезпекових організацій та дослідників. Це стало особливо помітно під час конференції RSAC 2024. Дослідники з аналітичного центру CSIS демонструють, як ШІ може впливати на процес прийняття рішень у сфері національної безпеки. Поки Китай і США планують значні інвестиції у дослідження ШІ (Китай – 50 мільярдів доларів, США – 39 мільярдів доларів) та розпочинають діалог на високому рівні з цього питання, фахівці з кібербезпеки вже стикаються з новими викликами.

Наприклад, фахівці з кібербезпеки Unit42 навчили ШІ створювати дієве зловмисне програмне забезпечення, використовуючи релевантну базу вихідних даних. Створене ШІ ПЗ виявилось не лише ефективним, але й здатним оперативно модифікуватися, створювати численні варіації та адаптуватися для різних платформ. Фахівці з Horizon3.ai вже пропонують нові сервіси з підтримкою ШІ для пришвидшення визначення пріоритетів кіберзахисту та усунення вразливостей у кібербезпеці організацій.

ШІ стає також об'єктом кібершпигунства. У травні невідома APT-група атакувала американських дослідників ШІ, намагаючись отримати доступ до їхніх даних. У червні 2024 року CISA провела перші командно-штабні навчання, присвячені загрозам від ШІ, та офіційно висловила занепокоєння щодо можливого впливу ШІ на зростання кіберзагроз у хімічному та біологічному секторах.

Одночасно з цим урядові структури США шукають способи застосування ШІ для підвищення безпеки. Міністерство оборони США наразі розглядає можливості використання ШІ для оперативного реагування на кібератаки.

Тенденції та прогнози

Сектор операційних технологій (ОТ) намагається адаптуватися до нової реальності підвищених кіберзагроз, що постають перед цією унікальною сферою. Занепокоєння щодо низьких стандартів кібербезпеки, від яких залежать критично важливі послуги економіки, зростає. Уряд США активно вирішує цю проблему, вдаючись до додаткового регулювання, проте власники промислових об'єктів вказують на системні проблеми з регуляторним процесом, який є здебільшого фрагментарним та суперечливим у контексті секторальних стандартів. Вони також зазначають, що ОТ є специфічними технологічними рішеннями, які складно і дорого модернізувати.

Однак, ці аргументи, ймовірно, не матимуть значного впливу, оскільки багато промислових організацій не дотримуються навіть найпростіших стандартів кібербезпеки, таких як заміна стандартних паролів. Це ставить під загрозу функціонування критичної інфраструктури. Подібна ситуація спостерігається у секторі водопостачання: через низку успішних кібератак за останні пів року Агентство з охорони навколишнього середовища США (EPA) провело перевірки, які виявили, що понад 70% систем водопостачання не відповідають Закону про безпечну питну воду та мають критичні кіберврразливості.

На цьому тлі продовжуються активні дискусії щодо необхідності повної заборони виплат викупів хакерам-здирникам. Проте, це питання викликає спротив з боку деяких стейкхолдерів, які занепокоєні тим, що такі обмеження можуть поставити під загрозу їхнє функціонування у випадку кібератаки. Зловмисники, зі свого боку, все частіше вдаються до нестандартних засобів тиску, включаючи фізичний тиск на потенційних жертв атак, як це відбулося у випадку з діяльністю групи UNC3944.

Підхід Secure by Design набуває все більшої ваги в державній політиці ключових країн. CISA активно просуває свою платформу Secure by

Design Pledge – добровільну ініціативу, яка об'єднує компанії, що беруть на себе зобов'язання дотримуватися принципів Secure by Design. Великобританія також готується до впровадження цього підходу для учасників ринку.

Технічний директор британського NCSC Оллі Вайтхаус зазначає, що нинішній підхід «тисячі пластирів» щодо кібербезпеки, коли розробники ПЗ або технологій точково вирішують конкретні проблеми кібербезпеки у своїх продуктах, має змінитися. Це стосується і соціальної відповідальності компаній-розробників перед своїми клієнтами, особливо структурами з традиційно обмеженими бюджетами на кібербезпеку, такими як НУО та школи.

На користь більшої безпеки при розробці ПЗ свідчить і важливий випадок, що стався у квітні, коли інфраструктура ПЗ з відкритим кодом, яка базується на використанні відкритих бібліотек, могла стикнутися з глобальною загрозою через складну та добре підготовлену спробу компрометації бібліотеки XZ Utils невідомими злочинцями. Загрозу випадково виявив співробітник Microsoft. Цей інцидент актуалізував питання безпеки використання продуктів з відкритим кодом та зміни підходів у цій сфері на користь більшої безпеки застосунків.

Людський фактор залишається одним із ключових джерел кіберзагроз для організацій та їхніх інформаційних систем. Це підтверджують квітневі дослідження Verizon та Proofpoint. За результатами опитування Verizon, 68% порушень безпеки сталися через не зловмисний людський фактор, тобто інциденти, пов'язані з інсайдерськими помилками або жертвами соціальної інженерії. Аналогічну статистику надає компанія Proofpoint. Ця проблема має більш масштабний характер, ніж просто навчання персоналу, і пов'язана із загальним рівнем кіберобізнаності. У зв'язку з цим, CISA у травні 2024 року запустила вже другу загальнонаціональну програму з підвищення кіберобізнаності. Програма охоплює різні цільові аудиторії, а інформація кампанії поширюватиметься на всіх основних платформах та майданчиках: телебачення, радіо, цифрова реклама, торгові центри, соціальні мережі та зовнішня реклама.

Протягом другого кварталу 2024 року відбулося лише кілька значущих кіберінцидентів, але обидва вони підкреслюють серйозні проблеми у сфері кіберзахисту охорони здоров'я. У США майже три місяці вирішували наслідки атаки на UnitedHealth, а в червні жертвою стала британська компанія Synnovis, яка займається клінічними дослідженнями і є ключовим партнером Національної служби здоров'я (NHS). За припущеннями, російські хакери атакували цю медичну установу, вимагаючи викуп у розмірі 50 мільйонів доларів. Британські

правоохоронні органи все ще розслідують цей інцидент, який, ймовірно, призведе до змін у кібербезпековій політиці Великобританії у сфері охорони здоров'я. Загалом, сектор охорони здоров'я залишається однією з найулюбленіших цілей хакерів, адже медичні заклади часто мають слабкі системи захисту та зберігають велику кількість персональних даних. Особливо вразливими є локальні медичні заклади, які часто мають обмежені ресурси для забезпечення належного рівня кібербезпеки.

Сполучені Штати Америки

Другий квартал 2024 року став часом значного кіберінциденту для США, пов'язаного з атакою на Change Healthcare. За масштабами цей інцидент порівнюють із Colonial Pipeline, але у медичному секторі. Хакери вкрали значний обсяг персональних даних клієнтів компанії, що призвело до того, що генеральний директор свідчив перед Палатою представників США. Розслідування та слухання у Сенаті виявили, що компанія виплатила викуп у розмірі 22 мільйонів доларів. Були також виявлені численні недоліки у політиці кібербезпеки, включаючи слабкий захист персональних даних та невідповідність кадрової політики щодо кібербезпекового керівництва (CISO організації була людина без досвіду роботи в кібербезпеці). Загальні втрати організації вже перевищили 800 мільйонів доларів і, за попередніми оцінками, можуть досягти одного мільярда. Цей випадок, ймовірно, призведе до посилення кібербезпекових вимог у всьому медичному секторі США та розробки відповідних стандартів, що може бути ускладнено через недофінансування NIST, агенції, яка займається розробкою цих стандартів.

США продовжують ротацію фахівців з кібербезпеки та розширення кібербезпекового блоку. На тлі запиту Білого дому щодо кібербезпекової складової бюджету на 2025 рік у 13 мільярдів доларів, було призначено нового директора з кібербезпеки в АНБ та створено департамент кіберполітики в Пентагоні. АНБ та CISA продовжують випускати рекомендації з безпеки, зокрема щодо впровадження Zero Trust. Водночас кількість інцидентів зростає. У квітні пройшла хвиля кібератак на муніципальні ресурси, міські IT системи та водний сектор США, в яких були виявлені зусилля російських кіберугруповань.

Це логічно призводить до підвищення уваги уряду США до освітньої складової через значну нестачу кіберфахівців у всіх секторах економіки (близько 500 тисяч незаповнених вакансій). Офіс національного кібердиректора США (ONCD) активно просуває імплементацію

Національної стратегії кіберосвіти та робочої сили, проводячи дискусії з учасниками ринку. Все частіше лунають думки про відмову від вимоги вищої освіти при наймі кіберфахівців на користь підтвердженої кваліфікації, що має допомогти також Міністерству оборони, яке наразі має близько 27 тисяч незаповнених кібервакансій через бюрократичні проблеми.

Європейський Союз

Європейський Союз активно адаптується до нового, більш динамічного ландшафту кіберзагроз. Одним із ключових заходів є розробка Закону про космос, який включатиме положення щодо кібербезпеки. Це особливо актуально на тлі зростаючих зусиль державних та приватних компаній з освоєння космічного простору, зокрема через виведення супутникових систем на орбіту.

Крім того, ЄС готується до впровадження постквантової криптографії для запобігання нових кіберзагроз. Єврокомісія вже випустила рекомендації для країн-членів, які вказують на необхідність розробки відповідних дорожніх карт для цього переходу.

Німеччина, зі свого боку, планує створити окремий рід військ – кіберсили, щоб швидше реагувати на нові загрози та посилити свою кібероборону.

Кібербезпека в Україні

У цьому кварталі Україна зосередила увагу на різних аспектах міжнародної співпраці та інтеграції до ЄС і НАТО. На першій науково-практичній міжнародній конференції з питань кібердипломатії, яка відбулася в Києві за підтримки НКЦК, Міністр закордонних справ Дмитро Кулеба підкреслив, що Україна, завдяки своєму досвіду протидії рф та репутацією новатора, є невід'ємною частиною європейської та євроатлантичної систем безпеки. Заступник Секретаря РНБО Сергій Демедюк закликав до спільної розробки стратегій для прогнозованого та постійного посилення колективної кіберстійкості.

Україна провела першу зустріч з представниками ЄС як країна-кандидат, зосереджену на питаннях цифровізації, зокрема на переговорному Розділі 10 «Цифрова трансформація та медіа». Міністерство оборони затвердило Основні засади інформаційної безпеки та кібербезпеки в інформаційно-комунікаційних системах, враховуючи найкращі підходи НАТО, міжнародні стандарти та практики з інформаційної та кібербезпеки. На третьому міжнародному засіданні Національного

кластера кібербезпеки було розглянуто питання поглиблення співпраці з ЄС та НАТО та обговорено практичні кроки, які Україна здійснює у сфері кібербезпеки.

Представники України взяли участь у кількох важливих міжнародних заходах. Керівниця служби з питань інформаційної безпеки та кібербезпеки Апарату РНБО України, секретар НКЦК Наталія Ткачук виступила на Asian Leadership Conference, де розповіла про досягнення України у розбудові національної системи кібербезпеки. На конференції RSA 2024 у Сан-Франциско українські представники поділилися зі світовою спільнотою експертів передовим досвідом країни у цій сфері. В рамках підписаного меморандуму, Україна та Польща домовилися про співпрацю у сфері цифрових технологій та інновацій, розвитку IT-індустрії, штучного інтелекту, електронного урядування, розвитку платформ «Дія» та mObywatel тощо.

У червні Національний координаційний центр кібербезпеки став партнером Paris Cyber Summit, а Україна вперше взяла участь у європейських кібернавчаннях Cyber Europe.

Україна активно вдосконалює та впроваджує державні політики у сфері кібербезпеки та новітніх технологій. Міністерство цифрової трансформації презентувало Білу книгу з регулювання штучного інтелекту, спрямовану на допомогу компаніям у підготовці до запровадження законодавчого регулювання у цій сфері та інтеграцію України до ЄС. Кабінет Міністрів України схвалив завдання Національної програми інформатизації. З метою автоматизації моніторингу виконання Стратегії кібербезпеки України, НКЦК презентував новий інструмент – CyberTracker. Державна служба спеціального зв'язку та захисту інформації затвердила вимоги до аудиторів інформаційної безпеки на об'єктах критичної інфраструктури та порядок їх атестації. Перший в Україні Кваліфікаційний центр інформаційних технологій та кібербезпеки розпочав сертифікацію спеціалістів у цій галузі. Україна підвищує кваліфікацію державних фахівців з питань кібербезпеки на всіх рівнях через регулярні навчання.

Фахівці команди CERT-UA продовжують моніторити тенденції у сфері кібербезпеки. У другій половині 2024 року вони зафіксували підвищений інтерес з боку ворожих хакерів до українського телекомунікаційного сектору. Атаки на військових, спрямовані на отримання доступу, контролю та викрадення розвідувальної інформації зі спеціалізованих систем ситуаційної обізнаності, залишаються стратегічною військовою ціллю противника. Серед груп, які здійснюють атаки на

Україну, найактивнішими є ті, що наразі не асоційовані з офіційними спецслужбами країни-агресора, хоча вони діють в інтересах російської влади.

Перша світова кібервійна

російські хакери продовжують атакувати союзників України, здійснюючи кібератаки на локальні муніципальні системи в США та впроваджуючи нові бекдори під час атак у Східній Європі. Група APT28 націлилася на польські інституції, а невстановлені російські хакери зламали сайт Польського агентства преси (PAP), розмістивши там фейкову статтю, що мала на меті погіршення україно-польських відносин. Ще одна успішна атака призвела до зламу сотні місцевих британських новинних сайтів.

У червні російські хакери атакували сайт іспанської компанії, яка ремонтує танки Leopard для України, втручалися у супутникові ефіри, що призводило до переривання трансляцій або навіть до показу російських військових відео на дитячих телеканалах. Вони також активно шукають нові інструменти доступу до жертв, наприклад, атакуючи компанію TeamViewer. Особливе занепокоєння викликає їхня готовність втручатися у виборчі процеси в США та Європі.

У травні відбулася серія дзеркальних кібератак проросійських та проукраїнських груп. 9 травня українським хакерам вдалося замінити сигнал з параду на деяких російських телеканалах на кадри з війни в Україні. У відповідь російські хакери зламали супутниковий сигнал телеканалу «Інтер» і транслювали українським глядачам російський парад.

Проукраїнське хакерське угрупування Blackjack успішно здійснило операцію проти інфраструктури російського «Москолектору». У червні російські енергетичні компанії, IT-компанії та державні установи стали жертвами трояна Decoy Dog, що спричинило збої в роботі супермаркетів по всій країні. Група Sticky Werewolf атакувала російську фармацевтичну компанію та науково-дослідний інститут, що займається мікробіологією та розробкою вакцин. Також було здійснено масштабну атаку на великі російські банки, що зробило їхні послуги недоступними для деяких користувачів.

У червні стало відомо, що прокурори Міжнародного кримінального суду розслідують ймовірні російські кібератаки на українську цивільну інфраструктуру як можливі воєнні злочини. Розслідування охоплює атаки, які поставили під загрозу життя цивільних, порушуючи електропостачання та водопостачання, перериваючи зв'язок зі

службами екстреного реагування або виводячи з ладу мобільні служби передачі даних, що передають попередження про повітряний наліт. Служба безпеки України також збирає докази на хакерів, які наприкінці 2023 року атакували оператора мобільного зв'язку «Київстар». Ці матеріали будуть передані до Міжнародного кримінального суду.

Паралельно з цим, російські хакери здійснюють атаки на українські бази даних і бази даних Міжнародного кримінального суду, намагаючись модифікувати або видалити докази воєнних злочинів, з метою переписати історію та уникнути післявоєнного правосуддя.