Глобальні тренди

У фокусі уваги 1 кварталу 2024 року – вразливість нульового дня Ivanti Connect Secure, яка стала інструментом для кібершпигунської діяльності китайського угрупування UNC5221. Вразливість, виявлена у січні 2024 року, залишається актуальною протягом всіх трьох місяців першого кварталу. За цей час ціла низка безпекових органів (американська CISA, британський Національний центр кібербезпеки, ENISA та CERT-EU, кібербезпекові агентства Альянсу Five Eyes) видали низку термінових директив та повідомлень для споживачів з різних секторів (починаючи від федеральних установ в США і закінчуючи промисловістю) аби зменшити масштаби проблеми. Загроза залишається актуальною, адже зловмисники можуть активно використовувати цю вразливість і підтримувати свою присутність в уражених системах. Зі свого боку АНБ США підтвердило, що вже зараз зловмисники, використовуючи цю вразливість, атакують підприємства оборонного сектору, а CISA була навіть змушена відключити декілька своїх систем аби не допустити кібератаки на них. З метою зниження загроз у стратегічній перспективі Пентагон оперативно затвердив окрему Стратегію кібербезпеки оборонно-промислового сектору.

Важливою подією кварталу стала вдала операція британських правоохоронців проти потужної ransomware групи Lockbit. На угрупування які використовують ПЗ-вимагач Lockbit припадає значна частина ransomware атак по всьому світу, і припинення їх діяльності дозволить зменшити негативну динаміку таких атак. Ці зусилля британських правоохоронців були доповнені діями української поліції, яка заарештувала двох учасників цього угруповання. Загалом, слід відмітити, що це вже другий помітний успіх правоохоронних органів у боротьбі з великими групами вимагачів – у 4му кварталі 2023 року американські правоохоронці припинили роботу іншого угрупування – Hive, і продовжують шукати його лідерів. Державний департамент США навіть оголосив винагороду за інформацію про них.

Незважаючи на помітні зусилля, ransomware залишається серйозною загрозою протягом усього звітного періоду. Середня сума початкового викупу від ransomware в 2023 році вже сягнула 600 тисяч доларів США, і зловмисники продовжують націлюватися на нові сектори, такі як сектор розваг та казино.

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.

Відносини між США та КНР в сфері кібербезпеки все більше набувають рис жорсткого суперництва, яке було характерне для першої декади 2000х років. У лютому 2024 року слухання перед Спеціальним комітетом Палати представників з питань Комуністичної партії Китаю висвітлили зростаюче занепокоєння безпекових органів США щодо китайської кіберактивності. В деяких з виступів звучали жорсткі оцінки дій китайських хакерських груп (наприклад, групи Volt Typhoon) які істотно відходять від дій кібершпигунства на користь прямих атак на об'єкти критичної інфраструктури чи створення там підготовчої позиції на випадок масштабного конфлікту (застосовуючи метод атаки "Living-Off-the-Land").

Вперше угруповання Volt Typhoon в травні 2023 року ідентифікувала компанія Microsoft. Кібербезпекові органі США разом з союзниками, такими як Австралія, Нова Зеландія, Канада та Великобританія у лютому випустили спільні настанови. В них йдеться, що Китай не лише збирає інформацію та займається шпигунською діяльністю, а проникає до мереж США та їх союзників з метою порушити функціонування критичної інфраструктури для створення хаосу, можливо в момент атаки Китаю на Тайвань. За словами очільниці CISA Джен Істерлі, після попередження та спільної операції різних країн, їх діяльність не припинилася. В березні було видано ще один документ з настановами, мета яких «надати керівникам об'єктів критичної інфраструктури вказівки, які допоможуть визначити пріоритети захисту критичної інфраструктури та їх функцій». Ще одна загроза від китайської кіберактивності – можлива атака на військову базі в Гуамі. Американські безпекові структури занепокоєні тим, що китайські кібератаки можуть мати дуже значний вплив на її функціонування.

Згадане загострення все частіше вибудовується не лише по лінії США-КНР, але і Європа-КНР. Особливо помітно це стало у березні 2024 року навколо цілої низки звинувачень на адресу китайських хакерських груп щодо втручання в роботу парламентських структур по всьому світу:

- Міністерство юстиції США оприлюднило висновок про те, що китайські хакери атакували європейських законодавців, зокрема членів Міжпарламентського альянсу з питань Китаю;
- британський уряд офіційно звинуватив Китай у кібератаках на демократичні інститути Великобританії;
- Фінляндія приписує злам фінського парламенту китайському угрупованню APT31;

- новозеландський уряд звинуватив КНР у кібератаках проти парламенту країни у 2021 році.

Вочевидь, така хакерська активність пов'язана і з тим, що в 2024 році в демократичних країнах відбуватимуться чисельні виборчі процеси, і країни занепокоєні можливим втручанням в них. Як відповідь - ENISA оновила довідник для забезпечення кібербезпеки виборчого процесу, а американська CISA відпрацювала процедури захисту виборчого процесу на прикладі «супервівторка[1]» у березні 2024 року.

Тенденції та прогнози

З огляду на ключову роль, що її відіграють супутники у світовій комунікаційній, навігаційній та безпековій системі, в США зростає занепокоєння кібербезпекою космічних об'єктів. Шириться розуміння, що вони можуть стати мішенню для кібератак противника, які можуть призвести до переривання сигналу, перехоплення, або повного відключення супутника. Щоб зробити реагування на проблему більш системним, CISA планує вивчити, чи є потреба в нових вимогах безпеки для космічних засобів, а також розширити можливості реагування на інциденти. Крім того, на випадок атаки, CISA має на меті посилити підтримку критичної інфраструктури, що залежить від можливостей космічного базування. Законодавці в Сенаті США представили проєкт закону для посилення кібербезпеки супутників, вимагаючи від CISA розробити відповідні онлайн-ресурси, а від Білого дому – створити федеральну стратегію боротьби з кіберзагрозами для супутникових систем. Втім, його розгляд знаходиться лише не початковому етапі.

Хоча дискусія щодо масштабів впливу штучного інтелекту на сферу кібербезпеки триває, майже всі організації вказують на нього як елемент, що змінює ландшафт кібербезпеки. Злочинці готуються використовувати генеративний ШІ (GenAI) з метою узагальнення тих даних, які вони вже вкрали і, фактично, створити нові вектори атак чи можливостей для вимог викупу. Захисники шукають можливості ширше використати ШІ для аналізу кіберзагроз. Водночас експерти вказують на певні концептуальні проблеми на цьому шляху, в т.ч. пов'язані із масивами даних, на яких відбувається навчання ШІ. Національний центр кібербезпеки Великобританії вважає,

[1] Супервівторок – день, в який велика кількість американських штатів одночасно голосує на праймериз, щоб визначитись з кандидатами у президенти від двох основних політичних партій США.

що протягом наступних двох років збільшиться обсяг застосування ШІ і посилиться його вплив на кібератаки.

Проблеми квантових обчислень та постквантового шифрування знову турбують безпекові структури. В той час як НАТО прийняло свою першу квантову стратегію, кібербезпекові органи європейських країн звертають увагу на необхідність приділити цьому питанню більше уваги і не відволікатись на підходи, які є сумнівними з точку зору ефективності (як то QKD). АНБО США починає відкриті дискусії щодо майбутнього квантових обчислень і як це вплине на сферу безпеки, а IBM вважає, що в 2024 році стане більше кібератак з метою крадіжки зашифрованих даних в надії отримати доступ до їх вмісту із появою квантових комп'ютерів.

Занепокоєння урядових структур щодо наступальних дій в кіберпросторі торкнулись і комерційного сектору. В лютому Великобританія та Франція спільно провели першу установчу конференцію, присвячену боротьбі із загрозою комерційного кіберрозповсюдження – тобто безконтрольного поширення з протиправною метою створених комерційними фірмами інструментів, які можуть використовуватись в наступальних кібердіях. За результатами учасники підписали декларацію Процесу Pall Mall, яка фіксує плани учасників ініціативи вивчати альтернативні політики та інноваційні методи боротьби з цією загрозою. Наразі Ізраїль майже не бере участі у цих ініціативах, адже ізраїльські компанії мають значну частку на експортному ринку шпигунського ПЗ.

Загрози кібербезпеці ОТ не лише не зменшуються, але стають все більш системними. Виробники обладнання та ОТ рішень все частіше знаходять нові вразливості у своїх продуктах - лише у лютому Siemens виявив 275 вразливостей у своїх виробах які активно використовуються в сфері автоматизації виробничих процесів. Звіт Dragos Inc підтверджує, що зловмисники все інтенсивніше входять в цю відносно нову сферу - у 2023 році додалось ще три кіберугрупування які націлені саме на ОТ інфраструктуру (Dragos наразі відслідковує 21 таке угрупування). Проблеми є не лише з виявленням вразливостей, але і з спробами їх виправити - дослідження показали, що організації з системами ОТ часто знають про недоліки, які використовуються в їхньому середовищі, але вони не можуть вирішити проблему оскільки гарантійний термін дії деяких застарілих систем закінчився, а особливості технічних процесів чи бізнес інтереси можуть ставати на заваді оновленню цих активів до найновіших операційних систем.

Інциденти з фізичною безпекою підводних кабелів можуть мати довгострокові наслідки для глобальної доступності мережі інтернет. У цьому кварталі увагу до теми підводних кабелів привернув інцидент, під час якого чотири основні підводні кабелі передачі даних, що обслуговують Африку, були сильно пошкоджені в районі Кот-д'Івуару лише через кілька тижнів після того, як поблизу Ємену був розірваний інший кабель. Це вплинуло на доступ до інтернету в Африці, а, також, на обмін даними між Африкою та Європою. Для запобігання таким наслідкам Європейська комісія видала Рекомендації щодо безпеки та стійкості підводної кабельної інфраструктури, в яких, серед іншого, йдеться про покращення координації всередині ЄС, як з точки зору управління, так і з точки зору фінансування.

Сполучені Штати Америки

На тлі зростаючого стратегічного протистояння США та Китаю в США зростає занепокоєння через наявність китайських компонентів у їх портовій інфраструктурі. За інформацією американського уряду, 80% кранів типу «судно-берег», що переміщують товари в портах США, виготовляються в Китаї. Розслідування Конгресу щодо вантажних кранів китайського виробництва виявило комунікаційне обладнання, яке, як видається, не є необхідним для підтримки їх нормального функціонування, і це може становити прихований ризик для національної безпеки. В той час, як конгресмени направили листа китайській компанії-виробнику цих кранів з вимогою пояснень, у лютому Президент Байден оголосив про намір видати виконавчий указ, спрямований на зміцнення безпеки та кібербезпеки американських портів, який розширюватиме повноваження Міністерства внутрішньої безпеки у цій царині.

Після низки кібератак проти систем водопостачання та водовідведення США та Великобританії у грудні 2023 року, організації, які за них відповідають, опинились у центрі уваги як безпекових органів, так і законодавців. При цьому атаки на цей сектор не припиняються – у січні була атакована британська Southern Water, що надає послуги водопостачання 2,5 мільйонам споживачів і послуги водовідведення 4,7 мільйонам клієнтів у південних регіонах Англії. Вже у середині січня CISA разом з партнерами опублікували Керівництво з реагування на інциденти для сектору систем водопостачання та водовідведення яке має допомогти організаціям побудувати свій кіберзахист. Проте власники таких кампаній кажуть, що у них часто взагалі відсутні ресурси на заходи кіберзахисту. В процес включився і Білий Дім, оголосивши про плани створити нову робочу групу, метою якої є захист

водного сектора від кібератак, спонсорованих державами. Працюють над цим питанням і аналітики, які пропонують державі запроваджувати заходи підтримки та стимулювання, щоб допомогти компаніям забезпечити належний рівень кіберзахисту.

Лютий та березень 2024 стали випробуванням і для американської системи охорони здоров'я. Наприкінці лютого відбулась атака хакерів Blackcat проти систем Change Healthcare (частина UnitedHealth Group), яка обробляє близько 50% медичних вимог (страхування) у Сполучених Штатах, що включає в себе близько 900 000 лікарів, 33 000 аптек, 5 500 лікарень і 600 лабораторій. Ця атака призвела до негативних наслідків для всієї системи охорони здоров'я країни, яка сильно залежить від страхування. Міністерство охорони здоров'я оголосило про початок розслідування інциденту, а Держдепартамент США оголосив про винагороду в 10 млн. доларів за інформацію про угрупування Blackcat. Ця атака сталась на фоні дискусій про необхідність посилення вимог щодо заходів кібербезпеки в медичному секторі - аж до висловленої в січні 2024 року ідеї пов'язати надання бюджетного фінансування лікарням з підтвердженням ними впровадження заходів кібербезпеки. Взагалі, атаки проти лікарень стали повсякденним явищем, так само як і викрадення даних пацієнтів. Зловмисники шукають все нові інструменти навіть не для проведення атак, а змушення атакованих до виплати викупів, шантажуючи не лише атаковані організації, але і пацієнтів. Федеральна влада ставиться до таких виплат все менш лояльно. Паралельно навіть приватні компанії (наприклад, Palo Alto Network) починають випускати настанови для закладів охорони здоров'я.

Європейський Союз

ЄС завершує процес прийняття Акту про кіберстійкість (Cyber Resilience Act) який має істотно змінити безпекові правила у всьому ЄС. Це доповнюється розробкою заходів з регулювання використання ШІ - Європарламент планує ухвалити Закон про штучний інтелект що передбачатиме регулювання ШІ на основі потенційних ризиків та впливу. В т.ч. як основні зусилля керівництва ЄС зосереджені на побудові кіберзахисту, аналітики оцінюють, як саме чинні кібербезпекові структури (такі як CSIRT) можуть бути більш корисними в загальноєвропейському контексті забезпечення кібербезпеки. Серед основних висновків – ці організації мають стати більш проактивними у своїй діяльності.

Також у 1 кварталі запрацювала перша європейська схема сертифікації для продуктів ІКТ відповідно до Загальних критеріїв. Схема включає в себе

елементи різних національних схем сертифікації і має на меті зробити використання ІТ продуктів європейськими споживачами більш безпечним. Наразі схема лише в процесі впровадження, але ЄС покладає значні надії на неї та подальший розвиток.

Кібербезпека в Україні

У березні 2024 року відбулась зміна керівництва Ради національної безпеки та оборони України – ключового координуючого та контролюючого органу України в т.ч. в сфері кібербезпеки. Під час представлення новопризначеного Секретаря РНБО Олександра Литвиненка саме інформаційна та кібербезпека були визначені Президентом України серед п'яти нових пріоритетів. Як вважає заступник Секретаря РНБО України Сергій Демедюк, з огляду на свій досвід у кібервійні з рф, Україна вже не є полігоном для відпрацювання можливостей рф, а може і має стати регіональним лідером із кібербезпеки, ініціюючи зміни у міжнародних підходах до агресії у кіберсфері.

Ворожа кіберативність проти українських ІТ систем продовжується. У січні було здійснено декілька особливо потужних кібератак – одна з них була спрямована на банківський центр, а інша помітно вплинула на один з найбільших дата-центрів України. Останнє призвело до порушення доступності послуг декількох державних організацій та інформаційних систем. Російські хакерські групи продовжують проводити кібершпигунські операції проти України (зокрема, одну з таких атак проти українських військових відслідковує компанія Securonix Threat Research), атакують урядові сайти (як, наприклад, сайт Міністерства освіти України), а також сферу медіа.

Загалом ці дані корелюються з загальним підвищенням кібератівності росії проти українських інформаційних систем – за даними Держспецзв'язку кількість кіберінцидентів минулого року зросла на 62,5%, а кількість кіберінцидентів, опрацьованих CERT-UA за минулий рік зросла на 15,9% у порівнянні з 2022 роком та склала 2543 кіберінциденти. Найпоширенішими типами інцидентів є розповсюдження шкідливого ПЗ, фішинг, шкідливе підключення, компрометація облікового запису та компрометація системи. Зловмисники традиційно проводять розвідувальні операції, вдаються до довготривалого шпигунства та знищення даних та інформаційних систем.

Як відповідь, Україна завдає контрударів (як, наприклад, дії військової розвідки України проти одного з російських постачальників ІТ систем для промисловості). У першому кварталі 2024 ГУР розповів про атаку на

російську систему управління дронами, що призвело втрати росіянами доступу до серверів. СБУ також наголосила на важливості інформації, зібраної кібершляхом, для здійснення складних кінетичних операцій. У березні Українські кіберфахівці здійснили низку успішних атак на ресурси країни-агресора. В результаті дій групи хакерів "UA25" було вивантажено 5 терабайт особистої і корпоративної конфіденційної інформації (в т.ч. матеріалів логістики по рф, матеріалів адвокатів та даних з деяких маркетплейсів). Головне управління розвідки між 11 та 18 березня 2024 року також атакувало приватні та державні структури, які фінансують війну проти України. Зазначається, що збитки від цих атак можуть сягати сотень тисяч доларів. ГУР також здійснило успішну спецоперацію проти Міноборони рф, під час якої отримано доступ до серверів та масиву секретної документації. Кіберфахівці СБУ зупинили поставки комплектуючих для російських дронів та крилатих ракет, а також працюють на фронті над знищенням ворожих систем РЕБ і РЕР та перехопленням безпілотників, які координують ракетні та артилерійські удари по Силам оборони.

Ці зусилля доповнюються традиційними заходами виявлення та затримання кіберзлочинців. Так у лютому було затримано двох міжнародних злочинців, а у результаті спільної операції Служби безпеки, правоохоронних органів США, Великої Британії, Євросоюзу та інших країн-партнерів викрито учасників потужного міжнародного угруповання вимагачів LockBit. Для попередження нових масштабних атак українські кіберфахівці активно вивчають наслідки масштабної кібератаки 2023 року проти телекомоператора «Київстар». За даними СБУ, російські хакери готували другу хвилю атак, яка мала нанести ще більше шкоди оператору.

Важливою є і співпраця з міжнародними партнерами – вже зараз Україна очікує на 13 млн. доларів кібердопомоги від Данії, USAID допомагає розбудовувати кібербезпеку енергетичного сектору, а CRDF Global – підвищує фаховий рівень кадрів національної системи кібербезпеки. Для налагодження стратегічних процесів координації спільних зусиль було запущено Талліннський механізм, перше засідання якого пройшло у Гаазі у середині лютого 2024 року.

Трохи раніше (7-8 лютого) у столиці України відбувся перший Київський міжнародний форум з кібербезпеки 2024: «Стійкість під час кібервійни», започаткований НКЦК при РНБО України разом з партнерами. Загалом у Форумі взяли участь понад тисяча учасників, серед яких топ посадовці України, США, ЄС та НАТО. Під час заходу відбулося 10 панельних дискусій і понад 40 експертних доповідей, які розкривали роль кібербезпеки

у сучасних війнах, досвід України у кібервійні, тему кібервійни і міжнародного права, кібердипломатії, посилення стійкості національної системи кібербезпеки через освіту, захищеність месенджерів, роль розвідки кіберзагроз, кібербезпека регіонів та інші. Також в рамках KICRF відбулись змагання з кібербезпеки, у яких взяла участь 21 команда фахівців із державного і приватного секторів.

Перша світова кібервійна

Продовжуються атаки рф на широке коло цілей, пов'язаних і не пов'язаних з Україною. У січні атак зазнали декілька кібербезпекових компанії та відділи кібербезпеки великих компаній. Серед них - Microsoft, яка стала жертвою атаки російського державного нападника Midnight Blizzard. Обсяги кібервтручання групи Midnight Blizzard все ще не до кінця зрозумілі - наразі Microsoft підтвердила лише, що зловмисники змогли отримати доступ до деяких сховищ її вихідного коду та внутрішніх систем. Атака зачепила і деякі акаунти електронної пошти високопосадовців США, що змусило CISA проводити власне розслідування та вживати заходів для пом'якшення наслідків.

На початку лютого жертвою нападників став акаунт фірми Mandiant в мережі X. Протягом недовгого часу зловмисники використовували його для популяризації фейкових операцій з криптовалютою.

Поштові скриньки кібербезпекового відділу технологічного гіганту HP Enterprise також стали жертвою атаки хакерів, пов'язаних із кремлем.

У лютому стало відомо, що російське кіберугрупування Turla починаючи ще з грудня 2023 року атакувало польське НУО яке підтримує Україну. Станом на березень кібербезпекові компанії продовжують дослідження цієї операції.

Російські хакери також націлились на політичні партії Німеччини та активно тестують вайпер AcidPour (модифікація AcidRain, що був застосований на початку військового вторгнення проти модемів KA-SAT) - вірус, що має знищувати дані в ураженій системі. Схоже, що оновлений вірус націлений на системи під Linux x86 і міг бути використаний проти низки телекомоператорів в Україні. Увага саме до політичних партій може слугувати додатковим свідченням наміру рф активно втручатися у виборчі процеси у Німеччині.

Західні дослідники продовжують вивчати досвід російських дій у кіберпросторі та надають власні прогнози та рекомендації щодо запобігання їм. Так, видання CSO Online описує структуру та методи діяльності

проросійської хактивістської групи NoName057(16) та стверджує, що така організація може стати моделлю для кіберзлочинців майбутнього. Разом з тим, видання підкреслює, що поки що діяльність угруповання, яке концентрується в першу чергу на DDoS атаках, не становить серйозної загрози заходу. Дослідниця Моніка Келло стверджує, що публічна ганьба та санкції, яких сьогодні вживають західні уряди, намагаючись впливати на дії рф у кіберпросторі, не є ефективним. На її думку, відповідь має ґрунтуватися на російській стратегічній культурі та включати прозорі розслідування наслідків російських операцій злому та витоків, та використовувати недовіру, яка панує в російських спецслужбах і суспільстві, щоб внести «тертя» в операційне середовище супротивника.