Глобальні тренди

Глобальне суперництво між США та Китаєм в цифровому просторі триває. Китайські APT-групи активізують кібершпигунські операції, при чому як проти державних організацій (як, наприклад, велика кампанія проти державних установ Камбоджі), так і приватного сектору (зокрема, проти групи компаній-виробників напівпровідників у Східній Азії). RAND Corporation у своїх дослідженнях вказує на те, що саме конкуренції між США та Китаєм за цифрову інфраструктуру буде матиме вирішальне значення для військових сил та операцій в регіоні. Одночасно Китай розширює свої стратегічні цілі та виявляє все більше цікавості до критичної інфраструктури. Реальність цієї загрози підкріплюється результатом дослідження компанії Fortress Information Security, яка продемонструвала, що майже все програмне забезпечення, використовуване енергетичними компаніями США, містить код від російських і китайських розробників та з великою вірогідністю має критичні вразливості, які можуть знаходитися в режимі очікування понад 4 роки. Органи безпеки США (NSA, CISA, Міністерство оборони) попереджають, що у разі кінетичної атаки на Тайвань, можливою є одночасна атака на ОКІ США, особливо об'єкти військової критичної інфраструктури. Крім того, кібердіяльність Китаю тепер також поширюється на операції впливу з використанням штучного інтелекту та дезінформації. Компанія Мета інформує, що як Китай так РФ будуть мережі он-лайн впливу напередодні виборів у США.

Загрози критичній інфраструктурі – постійний елемент загального ландшафту кіберзагроз. Такі організації продовжують залишатись бажаною ціллю для зловмисників, адже вони мають кошти і не можуть дозволити собі перерви в діяльності. Хоча більшість атак приходиться на IT системи таких організацій за допомогою ransomware (75% організацій у промисловому секторі зазнали атаки програм-вимагачів минулого року), однак це все одно впливає на основні функції організацій - вчасне постачання, взаємодія з клієнтами і т.д.. Однак вдалі кібератаки проти австралійського порту чи зі станцій муніципального управління водопостачання – лише частина проблеми, адже зловмисники все інтенсивніше шукають можливість атакувати промислові системи – не лише IT системи власників, але OT середовище. Це створює особливу проблему, адже в багатьох випадках OT системи захищені значно гірше ніж IT, а оновлень безпеки для багатьох контролерів просто не існує. Власники промислових систем часто

Ця публікація стала можливою завдяки підтримці, наданій Агентством США з міжнародного розвитку, згідно з умовами гранту Української фундації безпекових студій в рамках Проекту 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.

неуважні до кіберзагроз (про що свідчить майже 100 000 промислових систем керування, відкритих для публічного Інтернету), а вразливості для таких систем з'являються все частіше (це доповнюється виявленням нових 0-day вразливостей в промислових маршрутизаторах). Лише за звітний квартал з кібербезпековими рекомендаціями щодо різних аспектів кібербезпеки ОТ вийшли CISA (рекомендації щодо безпеки ОТ з відкритим кодом, а також регулярні повідомлення про виявлені нові вразливості), NSA (оприлюднення репозиторію OT Intrusion Detection Signature and Analytics) і це лише частина активності. Навіть приватні кібербезпекові організації як то Dragos в межах своєї програми Community Defense Program надають безкоштовні інструменти малим організаціям аби посилити кібербезпеку їх ОТ-інфраструктури. Наразі Україні відсутня чітка оцінка того, скільки промислових об'єктів мають ОТ-системи які можуть бути потенційно уражені зловмисниками, а також мають традиційний брак фінансових ресурсів для їх захисту. Тому пошук і приєднання до програм типу Community Defense Program можуть бути проміжним рішенням не лише для західних компаній, але і для українських.

Тенденції та прогнози

Останній квартал року – традиційний час для підведення підсумків та прогнозів. Протягом кварталу з'явились прогнози від компаній Proofpoint, Trellix та Trendmicro. Попри різні акценти компанії відзначають:

- зростання загроз від ШІ (його використання зловмисниками для організації фішингових атак, голосове шахрайство), що в свою чергу має стимулювати компанії серйозно розглядати етичні наслідки від використання ШІ та його впливу конфіденційність;
- фішингові атаки проти мобільних пристроїв;
- підвищену увага злочинців до облікових записів користувачів;
- у зв'язку з майбутніми виборами в США існує підвищений ризик кібератак на виборчі системи, бази даних виборців та виборчу інфраструктуру;
- приховані атаки на периферійні пристрої стануть частішими.
- дефіцит кіберталантів у сфері кібербезпеки буде зростати, хоча організації можуть зменшити цей розрив, підвищивши кваліфікацію своєї поточної робочої сили;
- широкомасштабні атаки ransomware продовжуватимуть зростати, оскільки вони забезпечують дуже високу віддачу від інвестицій для суб'єктів загрози.

Ці прогнози доповнюються оцінками британський NCSC який зазначив, що ОКІ зіштовхуються із «тривалою та значною загрозою» на тлі зростання сил державних угруповань, а також як наслідок зростання загальної агресивної кіберактивності та нових геополітичних викликів. Загалом все більше компаній відзначають зростання уваги зловмисників до соціальної інженерії. Хоча «атаки на людину» і раніше були ключовим методом на початкових стадіях кібератак, однак ШІ дав новий поштовх цій діяльності. Можливості ШІ у створені більш достовірних фішингових імейлів, імітації голосу і навіть відео людей, поява можливості динамічного управління великою кількістю акаунтів в соціальних мережах – істотно змінює ландшафт загроз.

Інша частина оцінок стосується підведення перших підсумків року, що минув. Першими з такими оцінками вийшли компанії Trendmicro яка зауважує наступне:

- вплив штучного інтелекту (зокрема, ChatGPT) на кібербезпекову ситуацію був перебільшеним (помітним був лише вплив в сфері фішингу);
- технології блокчейну зайняли свою скромну нішу виключно у фінансовому секторі і перестали сприйматись як проривна технологія в сфері кібербезпеки;
- збільшення кількості різних інструментів кібербезпеки в одній установі часто веде до більших проблем аніж до більшої безпеки, адже ускладнює їх адміністрування фахівцями організацій;
- хоча люди залишаються слабкою ланкою в сфері кібербезпеки, однак цьому сприяє загальна негативна культура в організаціях, яка не заохочує людей сповіщати про кібербезпекові проблеми;
- організації погано (нереалістично) формують запити на фахівців з кібербезпеки, що ускладнює їх пошук і формує брак робочої сили.

Сполучені Штати Америки

У IV кварталі 2023 року відбулось декілька подій, що матимуть довгострокові наслідки для кібербезпекової політики США. Передусім це призначення нових керівників для двох важливих кібербезпекових структур. Екс-співробітник ЦРУ Г.Круккер (Harry Coker) став Національним кібердиректором, а генерал-лейтенант Т.Хо (Timothy Haugh) змінив на посаді CYBERCOM і NSA генерала армії США Пола М. Накасоне, який очолював ці два відомства з 2018 року. Ці зміни відображають і зміни в політиці цих структур. В т.ч. як офіс Національного кібердиректора все більше зосереджується на імплементації Стратегії кібербезпеки США та Стратегії розвитку трудових кіберресурсів, NSA все частіше виступає із настановами орієнтованими на

широке коло організацій в середині США, а також нарощує свої міжнародні контакти – вони є постійними учасниками партнерських проектів в межах Альянсу п'ять очей. Ці призначення відбуваються на тлі більш широкої дискусії щодо доцільності розділення NSA та CYBERCOM та продовження реформ у сфері кібербезпеки США у відповідності до настанов Solarium Commission. Поява у попередні місяці першого в американській практиці чіткого плану виконання Стратегії кібербезпеки США також вказує на те, що Білий Дім хоче докласти більше зусиль до контролю за цим документом, більш чіткого розуміння хто і за що відповідає при його реалізації, а також створити прозорий механізм визначення результатів його імплементації. Швидше за все новий очільник Офісу національного кібердиректора буде зосереджений саме на цій контрольно-координаційній функції.

Другий важливий фокус уваги – розвиток та регулювання Штучного інтелекту (ШІ). Так, наприкінці жовтня Президент США Дж. Байден підписав новий указ. На його реалізацію американська CISA вже оприлюднила власну Дорожню карту щодо того, як це ключове кібербезпекове федеральне відомство буде враховувати виклики ШІ у своїй діяльності, а спільно з NCSC Великобританії вони випустила спільні рекомендації щодо безпечної розробки системи ШІ. Все більш чітке позиціонування державних органів США в частині розвитку ШІ вказує на те, що вплив цих технологій на безпековий сектор США став настільки помітним, що змушує держави швидко самовизначатись із інструментами підтримки та контролю.

Третій фокус – продовження боротьби із вірусами-вимагачами (ransomware). Наразі США розглядає як наступний крок протидії не лише боротьбу з інфраструктурою злочинців чи конкретними групами, але і зміну поведінки жертв. Зокрема це стосується посилення заходів із недопущення виплати викупів аби не заохочувати злочинців до зловмисних дій. Поки що ці зусилля є лише частково успішними – ransomware групи продовжують досить успішну діяльність, атакуючи все нові цілі. В США під ударом залишається, передусім, сектор охорони здоров'я. Про недостатність уваги до власної кібербезпеки в цьому секторі свідчить той факт, що за даними компанії Sophos зловмисникам вдалося зашифрувати дані під час майже трьох чвертей атак.

Четвертий фокус – взаємодія з партнерами та впровадження архітектури нульової довіри. У відповідності до нової Стратегії кібербезпеки, США розширює коло партнерів по всьому світу, одночасно з цим шукаючи нові способи безпечно обмінюватись інформацією з найбільш довіреними

партнерами. Поряд з такими новинами, як укладання робочої угоди між ENISA та CISA, або про формування нового партнерства між США, Південною Кореєю та Японією, військові органи США шукають більше практичних шляхів взаємодії з акцентом на Тихоокеанський регіон. CYBERCOM США розширює практику спільних кібернавчань з партнерами в цьому регіоні, НАТО залучає Японію та Південну Корею до своїх навчань в межах Cyber Coalition 2023, а Пентагон будує спеціальну мережу Mission Partner Environment для обміну інформації з Філіппінами та Тайванем. Ці зусилля додатково посилені кібердопомогою, яку США через свій військовий бюджет планує надати Тайваню в найближчі роки – це чітко вказує на основні занепокоєння військового командування США в частині недопущення ще однієї ескалації військової ситуації у світі.

Новий тренд цього кварталу – кібератаки проти систем водопостачання на рівні окремих невеликих громад в США. За два місці відбулось щонайменше три таких атаки (відповідальність за них взяли пропалестинські угрупування на кшталт Cyber Av3ngers), а ще одна схожа сталась в Ірландії. Хоча компанії заявили про відсутність загроз для споживачів (частково постраждали користувачі лише в Ірландії), але факт атаки на промислову систему є сталою тенденцією спроб хакерів впливати на функціонування ОКІ. Ці атаки показали наскільки локальний рівень залишається не захищеним перед кіберзагрозами – там ще більш серйозно відчувається брак кадрів та фінансових ресурсів для належного кіберзахисту ніж на центральному рівні. Можна прогнозувати, що локальні/місцеві об'єкти критичної інфраструктури все частіше будуть ставати мішенню для зловмисників, які планують довести неспроможності центральної влади захистити всіх громадян.

Помітною тенденцією яка продовжується у звітному кварталі є все більша увага кібербезпекових структур по всьому світу до створення нових сервісних функцій та проактивне надання рекомендацій учасникам ринку. Наприклад CISA запускає нову програму обміну інформацією про кіберінциденти з приватним сектором, британський НКЦК щомісячно запроваджує або нові сервіси або пропонує власну експертизу для потреб приватного сектору (наприклад у звітному кварталі британський НКЦК запропонував перелік організацій, які можуть надавати кваліфіковано послуги з проведення ТТХ всіх рівнів). Очевидною є активізація кібербезпекових структур Альянсу п'ять очей які майже кожного тижня випускають спільні (а отже швидко погоджені) повідомлення про актуальні кіберзагрози – це є свідченням тісної щоденної взаємодії цих організацій, а отже – високого рівня довіри при обміні даними.

Європейський Союз

Європейський Союз після майже річних дискусій розпочав рух щодо прийняття Акту про кіберстійкість (Cyber Resilience Act). Цей документ створює нові рамки функціонування для IT сектору та виробників IT обладнання, вимагаючи від них більше уваги до заходів кібербезпеки. Швидше за все імплементація цього документу буде складною та відбуватись з різною швидкістю в європейських країнах. Про це каже і досвід впровадження NIS2 Директиви, яка більше ніж рік після свого прийняття все ще слабко імплементована у багатьох європейських країнах. При цьому ЄС чітко розуміє зростання ролі кібербезпеки і готовий залучати до цього кошти (остання ініціатива стосується залучення 214 млн. євро на кібербезпеку). Це доповнюється закликом керівництва ЄС до створення європейських кіберсил, що будуть мати наступальні можливості.

Складно не відмітити, що всі ці зусилля (в т.ч. готовність Брюсселю інвестувати в кібербезпеку) слабко корелюється з реальною ситуацією в сфері кібербезпеки на самих ОКІ. Звіт ENISA у листопаді 2023 року чітко вказує на те, що хоча кіберчастка IT-бюджету ОКІ досягла 7,1% у 2022 році, однак це лише на 0,4% більше ніж у 2021. Крім того, 47% ОКІ не планують наймати фахівців з кібербезпеки протягом наступних двох років, при цьому 83% організацій стверджують, що мають труднощі з наймом принаймні в одній сфері інформаційної безпеки. В попередні місяці ENISA публікувала схожі дослідження які показують аналогічні тенденції - власники ОКІ або не бажають інвестувати в кібербезпеку або не вважають це за потрібне. Враховуючи ці тенденції та загальний характер нормативних змін до яких вдається Єс останнім часом можна передбачити, що європейське законодавство в сфері кібербезпеки буде вставати все більш жорстким та ультимативним, а його порушення буде вести до значних штрафів для компаній (як це є в сфері застосування GDPR).

Як і США Європейський Союз, своєю чергою, планує провести оцінку ризиків, створених ШІ – результати цієї оцінки будуть використані при розробці нормативно-правової бази та політики для зменшення ризиків і зміцнення позицій ЄС у світовому технологічному ландшафті. Ця активізація зусиль ЄС обумовлена все ширшим використанням технологій на базі ШІ – від розробки нових програм до загроз автономним системам управління морським транспортом.

Російська кіберактивність

Російська кіберактивність не зменшується. В 2024 році відбудеться ціла низка виборів по всьому світу (включаючи США та Великобританії) і вже зараз безпекові органи відмічають, що APT групи з росії та КНР готуються до цих подій, плануючи втрутитись в них. Ця спрямована активність доповнюється дослідженнями сучасного ландшафту кіберзагроз, який каже, що більше ніж 60% DDoS атак наразі мають політичне підґрунтя, а фахівці з кібербезпеки вже прямо кажуть, що групам реагування на кіберінциденти доведеться слідкувати не лише за своїми інформаційними системами, але і геополітичними подіями які стають каталізатором нових загроз для державного та приватного секторів.

Не припиняється ворожа діяльність – лише у звітному періоді російська APT29 атакувала посольства по всій Європі, угрупування UAC-0165 намагалось втрутитись в роботу 11 українських провайдерів – ці дані доповнюються черговим звітом Держспецзв'язку, який відзначає, що кількість зареєстрованих кіберінцидентів у першому півріччі 2023 року зросла більше ніж удвічі.

Кібербезпека в Україні

Протягом жовтня-листопада 2023 року українським правоохоронним структурам вдалось провести декілька успішних операцій проти міжнародних груп кіберзлочинців. Один з найбільших успіхів – ліквідація угрупування, яке за допомогою використання ransomware заподіяла шкоду на 80 мільйонів доларів. Ці успіхи доповнюються іншими операціями Кіберполіції спільно з чеськими колегами, а також операцією проти групи, яка починаючи з 2020 року атакувала 168 компаній. Ця діяльність була помічена і на міжнародному рівні що корелює із занепокоєнням західних країн щодо загроз ransomware. Практичний внесок в протидію цій загрозі може сприяти додатковій розбудові довіри між Україною та країнами-партнерами, а також стимулювати започаткування більш системних спільних заходів у боротьбі з кіберзлочинністю.

Розвиток міжнародної співпраці залишається важливим вектором діяльності. У листопаді 2023 року Україна (НКЦК РНБО та ДССЗЗІ) підписали Робочу угоду про співпрацю з ENISA (Європейською агенцією кібербезпеки). Для ENISA це стало першою такою угодою з партнером з-поза меж ЄС. Підписання таких документів – важливий елемент на шляху формування глобальної кіберкоаліції для протидії загрозам, що походять із росії та інших держав, які стоять по один бік з агресором. Водночас слід відмітити, що важливим є наповнення цієї співпраці практичними кроками та заходами

з української сторони. Ефективність співпраці буде сильно залежати від готовності української сторони не лише запропонувати чітку дорожню карту співпраці, але і постійний рух по ній.

Україна продовжує протистояння з російськими кіберсилами. У грудні 2023 року відбулась серйозна кібератака проти одного з національних операторів мобільного зв'язку – Київстар. Наслідки атаки руйнівні – щонайменше декілька днів абоненти компанії не могли скористатись жодним зв'язком, а процес відновлення розтягнувся на декілька тижнів. Це доводить, що відсутність руйнівних кібератак протягом 2х років війни є не лише результатом ефективних кіберзахисних дій, але і можливо все ще не виявленими позиціями ворожих хакерів в інформаційних системах. Російські хакери все ще активні і синхронізують свої дії з загальною російською військовою стратегією (наприклад, атакуючи паралельно з ракетними ударами сільськогосподарський сектор України), при цьому APT групи які працюють проти України майже не змінюються. Можливо Україна потребує більш тісної координації кібербезпекових органів із основними телекомоператорами (схожий формат реалізовано у американської CISA у вигляді окремого комітету до якого входять представники CISA та гравці ринку телекому).

Українські кібербезпекові структури (Держспецзв'язку, СБУ) оприлюднили власні оцінки поточного українського ландшафту кіберзагроз в Україні та прогнозів на найближче майбутнє. Серед таких оцінок – зростання кількості складних атак на ланцюжки постачання, а компанії, які розробляють програмне забезпечення для критичної інфраструктури та військових, зазнаватимуть активних цілеспрямованих кібернападів у довгостроковій перспективі. З іншого боку вже зараз більшість ворожих кібератак спрямовані на доступ до електронного документообігу українських держустанов і технологічних систем інфраструктури. Саме тому СБУ та Держспецзв'язку звернули увагу енергетичних компаній на підвищені загрози кібербезпеці з боку росії у зимовий період. Базуючись на досвіді минулих років спеціальні служби вказують на вірогідність активних спроб російських хакерів вплинути на роботу об'єктів критичної інформаційної інфраструктури, енергетичної сфери та надання ними життєво-важливих сервісів. Хоча загрози через ланцюжки постачань традиційно визначаються як критичні для української кібербезпеки, однак досі відсутні прості та зрозумілі настанови як приватним компаніям чи державним органам убезпечитись від таких загроз. Ситуація ускладнюється тим, що таких організаціях часто відсутні досвідчені фахівці, які можуть самостійно опрацьовувати наявні міжнародні стандарти чи рекомендації в цій сфері.

Британські, американські та французькі кібербезпекові органи вирішують це питання шляхом підготовки спрощених рекомендацій та автоматизованих інструментів (як це зробила MITRE) які орієнтовані на не фахівців.

Україна продовжує нарощувати власні спроможності щодо реагування на кіберінциденти. Зокрема, розширює практику проведення кібернавчань (наприклад НКЦК проведено змагання з кібербезпеки HackWave та INCIDENT RESPONSE DAYS 2.0, а також відбулись перші секторальні кібернавчання для транспортного сектору CIREX.CoBridge), запускає нові інструменти кібергігієни (наприклад Мінцифра запустила тест на знання правил безпеки в мережі «Кіберграм», а ДССЗЗІ провела всеукраїнський онлайн-урок з кібербезпеки для понад 20 тисяч глядачів) та стимулює інновації в секторі кібербезпеки.

Перша світова кібервійна

Перша світова кібервійна триває й агресор не зменшує інтенсивність власних дій. При цьому відповідно до даних компанії Microsoft, у 2023 році авторитарні уряди (росії, КНР, Ірану та Північної Кореї) сконцентруватися на кібершпигунських операціях, намагаючись отримати більше інформації щодо важливих для них зовнішньополітичних ініціатив. Мішенню атак вищезгаданих акторів стають не лише західні компанії та уряди. Як стверджує російська державна компанія “Солар”, Китай і Північна Корея стали ключовими джерелами наступальних кіберкампаній проти росії у 2023 році.

Росія все частіше атакує міжнародних партнерів України, намагаючись завадити логістичними процесам, викрасти інформацію з дипломатичних установ, або атакуючи ОКІ. Більшість цих атак це все ще DDoS атаки таких угруповань як Killnet чи Anonymous Sudan, але все частіше до них підключаються APT групи. З огляду на те, що 2024 рік буде роком, в якому відбуватиметься найбільша кількість виборів у світі за всю попередню історію, очікується, що і виборча інфраструктура і передвиборчі дискусії стануть мішенню атак російських зловмисних акторів. Серед ключових - вибори Президента США, вибори до Європейського парламенту, вибори до нижньої палати парламенту Великобританії, вибори у низці інших ключових європейських країнах-партнерах України.

Атаки на КІ – все ще важлива мета російських кібероперацій. Про це свідчить і звіт Mandiant щодо кібератаки угруповання SandWorm на системи операційних технологій (ОТ) української енергокомпанії наприкінці 2022 року. Актор вперше використав методи OT-level liveing off the land (LotL), щоб, ймовірно, спрацювали автоматичні вимикачі підстанції жертви,

спричинивши незаплановане відключення електроенергії, яке збіглося з масовими ракетними ударами по критичній інфраструктурі по всій Україні. Кібератаки проти енергетики по всьому світу з боку російських злочинних груп – помітна тенденція, і такі дії стають все більш небезпечними. Прикладом є Данія, чиї 22 енергетичні кампанії зазнали скоординованої кібератаки у травні 2023 року. Підозрюється, що за цією атакою стоїть та ж Sandworm (APT28).

І Україна і країни-партнери не просто захищаються, але контратакують. В т.ч. як США традиційно намагається знищувати інфраструктуру злочинців та виявляти самих зловмисників (в т.ч. для введення проти них персональних санкцій), Україна проводить більш активні дії проти супротивника. У звітному кварталі вперше стало відомо, що українські спеціальні служби (ГУР МО) повідомили про проведення декількох успішних операції у кіберпросторі проти «росавіації» та центральних серверів Федеральної податкової служби РФ (включно з 2300 її регіональних серверів по всій Росії, а також на території тимчасово окупованого Криму). Перша атака дозволила здобути великий обсяг закритих службових документів росавіації. Друга - ліквідувати конфігураційні файли, які роками забезпечували функціонування розгалуженої податкової системи РФ - знищена вся база даних та її резервні копії. Це вказує на більш широке зміщення кібербезпекової дискусії з виключно сприйняття кіберпростору як простору нападу та захисту (що довгий час вважалось прийнятною нормою у всьому західному світі), як простору рівних змагань, де атаковані можуть завдавати контрударів і самі переходити у наступ.

У світі йде дискусія з приводу створення кіберсил, як окремого роду військ та їх інтеграції до ефективних спільних операцій з іншими родами. Так, до перегляду завдань оборонної сфери закликав начальник відділу оборонних інформаційно-комунікаційних технологій Міністерства оборони Австралії генерал-майор Мюррей Томпсон, підкреслюючи, що такий огляд в 1918 році призвів до створення військово-повітряних сил, які на той момент тільки почали відігравати значну роль у військових операціях. Про створення кіберсил йдеться і в Україні. Секретар НКЦК при РНБО України Н. Ткачук під час міжвідомчого заходу щодо «Забезпечення кібероборони держави» підкреслила необхідність якнайшвидшого створення українських кіберсил на основі досвіду України та успішних міжнародних кейсів. Президент Ради ЄС запропонував створити «європейські кіберсили» з «наступальними можливостями», але така пропозиція поки що не знаходить підтримки Міністрів оборони ЄС.