Війна в кіберпросторі і тренди кібербезпеки-2022

Пандемія, а потім вторгнення росії в Україну спричинили тектонічні зміни в ландшафті кібератак. Перша змусила людей працювати за межами периметру захисту, а друга розмила межу між солдатами на фронті і цивільними хакерами в тилу.

Кіберзахист — це війна броні та снаряду, у якій обидві сторони вигадують нові способи ошукати одна одну. Обидві застосовують машинне навчання і автоматизацію. Використання хмарних за стосунків і мобільних пристроїв розмило периметр корпоративної мережі, і ще більше змінив ситуацію змінив 2020 рік, коли персонал масово перейшов на віддалений режим роботи. А потім російсько-українська війна викликала зливу кібератак і змусила хакерів обирати сторону.

«МтБ» вирішив поглянути на останні зміни ландшафту загроз і тренди захисту від них. Також розповідаємо про кібератаки, до яких вдаються росіяни, і що їм можуть протиставити захисники.

Більше витрат, більше витоків

Для початку кілька цифр. Як прогнозував два роки тому журнал ***Cybersecurity Ventures***, глобальні збитки від кіберзлочинності до 2025 року сягнуть $10,5 трлн, порівняно з $3 трлн у 2015 році. При щорічному зростанні у 15% це буде найбільший в історії перерозподіл економічних багатств, щорічні збитки від кіберзлочинів на порядок більші за ті, що їх завдають стихійні лиха, а сам бізнес вже стає більш прибутковим, ніж торгівля усіма основними наркотичними речовинами разом узятими.

За даними консалтингової компанії ***Accenture*** станом на кінець 2021 року, 43% всіх кібератак спрямовані проти малого бізнесу, але лише 14% компаній готові захистити себе. Атаки не лише порушують діяльність підприємств, але й можуть пошкоджувати

Рис 1. Сектори економіки, що зазнали кібератак 1 кварталі 2022 року (джерело: Trellix)

важливі IT-активи та інфраструктуру, відновити які буває неможливо через брак коштів або інших ресурсів.

Згідно з обрахунками ***IBM***, у 2021 році середній витік даних розміром у 1000 — 100 000 облікових записів клієнтів коштував компаніям $4,24 млн. Подолання наслідків «мега-витоків» (50–65 млн записів) коштувало в середньому трохи більше $400 млн. Найсерйозніших збитків завдавали витоки у сфері охорони здоров'я (в середньому $9,29 млн), фінансових послуг ($5,72 млн) і фармацевтики ($5,04 млн). Як видно зі звіту ***Trellix*** (компанії, що торік утворилась внаслідок злиття McAfee та FireEye), у 1 кварталі нинішнього року на атаки проти медичної сфери надалі припадає суттєва доля серед загального числа (**рис. 1**).

За оцінками IBM, внаслідок пандемії близько 60% компаній перевели бізнес у хмару, аби продовжувати свою діяльність, проте не завжди це супроводжувалось посиленням захисту. Якщо мала місце віддалена робота, разові збитки від витоку даних зростали, в окремих випадках на приблизно на $1000.

Щоб виявити і зупинити витік даних, організації потребували в середньому 287 днів (на 7 більше, ніж у 2020-му), з них 212 днів витік лишався непоміченим. Однак компанії, які застосовували рішення захисту на основі штучного інтелекту, машинного навчання, аналітики і шифрування, зменшували потенційну вартість витоку в середньому на $1,25–1,49 млн.

Водночас, як зазначає кіберстрахувальна компанія ***Embroker***, витік даних може мати наслідки, які тривають багато місяців чи навіть років і спричиняють значні витрати, яких компанії навіть не передбачають у своїх планах (**рис. 2**). Ці кошти включають втрачені дані, порушення роботи підприємства, втрачені прибутки через простій, витрати на відшкодування і навіть удар по репутації бренду. Важливо

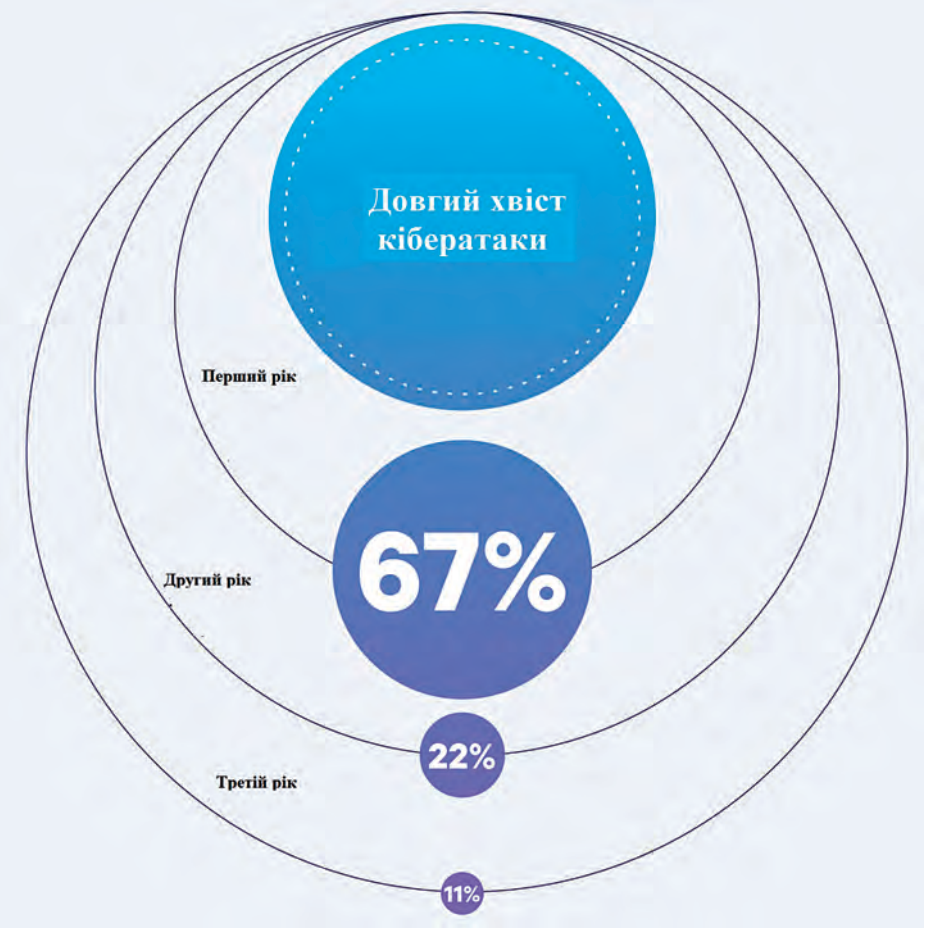


Рис. 2 «Довгий хвіст» збитків від витоку даних (джерело: Embroker)

мати стратегію управління ризиками для мінімізації негативного впливу витоків даних. Наприклад, план реагування на інциденти, який містить інструкції щодо кроків на етапах виявлення, ізоляції, розслідування, ліквідації наслідків витоку і відновлення нормальної роботи.

Від проблем ковідних років перейдемо до викликів, спричинених воєнними діями.

Перша світова кібервійна

Російсько-українська війна та її відлуння в кіберпросторі займають чільне місце у звітах компаній, що досліджують ландшафт кіберзагроз. ***Check Point*** відзначає: тоді як досі кіберзлочинні групи шукали здебільшого фінансової вигоди, російсько-українська війна спонукала кіберзлочинні колективи та індивідуальних хакерів зайняти той чи інший бік конфлікту. Trellix також вважає, що війна стала каталізатором, який спонукав злочинний світ розділитися. *«Історично кіберзлочинці часто оминали політику, і ми підозрювали, що багато російських та українських здирників працюватимуть разом заради фінансової вигоди»*, — йдеться у звіті компанії.

Вже на третій день російського вторгнення, 27 лютого, Check Point зафіксував збільшення числа кібератак проти державного і військового секторів України на 196%, а проти російських організацій — на 4%. У березні український CERT повідомляв про численні атаки проти об'єктів критичної інфраструктури — лише протягом одного тижня було зафіксовано 65 таких атак.

Російські хакерські групи приєднались до бойових дій одразу з початком війни, забезпечуючи «суттєву підтримку в кіберпросторі». Зокрема, угруповання ***APT28*** розпочало кампанію проти місцевих органів влади з метою викрадення тактичних і стратегічних даних. Група ***Conti*** вже 25 лютого оголосила про повну підтримку російського уряду і пригрозила атакувати критичну інфраструктуру кожного, хто діятиме проти росії. Проросійська група ***Killnet*** вчинила DDoS-атаки проти членів НАТО й інших держав, які підтримують Україну. Значним компонентом атак були програми-вайпери, призначені для негайного порушення функцій і знищення даних. За день до вторгнення було застосовано вайпери проти сотень об'єктів державного фінансового, IT– та енергетичного секторів України.

За оцінками Check Point, хакерські групи почали підготовку до операцій ще за кілька місяців до вторгнення військ РФ: проводили розвідку, розподіляли цілі і здобували доступ до стратегічно важливих постачальників. Водночас, хоча деякі групи явно пов'язані з російським ГРУ, невідомо чи існує між ними якась координація, чи просто хакерам було передано загальний список цілей.

Кіберстратегія України стала великою несподіванкою, йдеться у звіті Check Point. Росія має перевагу в кіберпросторі, оскільки там існує багато потужних хакерських груп, лояльних до Кремля і його спецслужб; проте на бік України стали різноманітні активісти, «білі хакери» і навіть знаменитий колектив Anonymous. Найцікавіше те, що сам уряд запросив на допомогу гравців «з обох сторін закону». Вже в перші дні війни міністр цифрової трансформації Михайло Федоров у Твіттері закликав «цифрові таланти» приєднуватися до новоствореної «IT-армії»; водночас прихильники України почали розміщувати заклики про допомогу на підпільних форумах. Мінцифри створило спеціальний Telegram-канал, де «цифрові воїни» отримують завдання; вже за три дні мав 175 тис. підписників. Додамо, що Trellix у 1 кварталі цього року зафіксував збільшення числа інцидентів у росії на 490% порівняно з 4-м кварталом 2021-го. Створення спонсорованого державою кібервійська є безпрецедентним кроком, зазначається у звіті Check Point.

Понад те, коли російсько-українська війна врешті закінчиться, ситуація буде гіршою, ніж до її початку, адже за час конфлікту всі ці спонсоровані державами угруповання, активісти та злочинці отримають нові навички та інструменти, також вони намагатимуться атакувати країни НАТО. Готуватися слід і бізнесу, адже кіберзлочинцям потрібні гроші для вербування і технологічного озброєння, а основні їхні прибутки походять саме від зламування підприємств.

Здирники на війні

Дослідники зауважують ще одну цікаву річ — метаморфози, які відбуваються з групами кіберздирників. Як пише Check Point, вони пройшли шлях від окремих осіб чи невеличких колективів, які розсилали навмання електронні листи, сподіваючись набрати малих викупів, до груп з сотнями «працівників», що оперують сотнями мільйонів чи навіть мільярдами доларів. Проте чим більша організація, тим важче їй приховувати свій бізнес, а отже, діяльність злочинців неможлива без сприяння чи хоча б пасивної згоди місцевої влади. Ця залежність змушує великі кіберзлочинні групи до роботи на геополітичні інтереси країн, де вони перебувають.

Після кількох гучних здирницьких атак уряд США та правоохоронні агенції світу розпочали скоординовану акцію, яка включала в себе санкції, боротьбу з відмиванням криптовалют та інші заходи. Росія в цьому брала участь «вибірково»; зокрема, у січні було затримано членів відомого угруповання ***REvil***, проте компанія ***AdvIntel*** вже тоді повідомляла, виходячи з аналізу обговорення у кіберзлочинній спільноті, що рейд ФСБ скоріше був піар-акцією, покликаною продемонструвати готовність співпраці з Заходом (саме тоді відбувалися російсько-американські переговори з безпеки). До того ж було заарештовано далеко не перших осіб — лише тих, які виконували допоміжні операції, такі як відмивання грошей. Check Point зазначає, що вже у квітні блог і Tor-мережа REvil знову запрацювали, що дивним чином збіглося з війною в Україні і кінцем співпраці між США та РФ.

Інша група, вже згадана Conti, настільки знахабніла, що почала нападати на цілі країни. У квітні вона зашифрувала дані щонайменше 27 урядових структур Коста-Ріки і зажадала викупу від цієї країни, а у травні атак зазнало Перу. 12 травня президент Коста-Ріки оголосив надзвичайний стан, а згодом заявив, що країна перебуває у стані

війни з Conti — це був перший випадок в історії, коли держава оголосила війну кіберзлочинній організації. Після того, як Коста-Ріка відмовилася платити викуп, Conti відкрито оголосила про намір повалити уряд і закликала жителів країни до повстань.

В результаті атаки на міністерство фінансів було зашифровано терабайти даних і виведено з ладу понад 800 серверів. Фактично було паралізовано усі експортно-імпортні операції, і довелось повертатися до паперових документів. Вже в перші дні здирницької кампанії, у квітні, втрати бізнесу оцінювались від $38 млн на день до $125 млн за 48 години. Друга хвиля вразила Фонд соціальної безпеки, який керує системою охорони здоров'я країни — було виведено з ладу половину з 1500 серверів і 10400 комп'ютерів, перенесено понад 34 тис. направлень до лікарів.

Аамір Лакхані, дослідних ***Fortinet***, вбачав у цій кампанії спробу Conti відновити свою репутацію, яку підмочили витоки внутрішніх даних цієї злочинної групи. Ці матеріали, оприлюднення яких стало помстою за підтримку росії, викрили структуру і організацію роботи Conti, а також код їхньої програми-шифрувальника. Conti, отже, намагалася довести, що залишається потужною і небезпечною силою.

Існує протилежна версія, згідно з якою війна проти Коста-Ріки була завершальним акордом складної операції з ребрендингу. Як вважають розслідувачі з AdvIntel, відкрита заява про підтримку дій РФ мала наслідки, які зрештою зробили подальший бізнес неможливим. По-перше, Conti порушила негласне правило російськомовної кіберзлочинної спільноти: не встрявати в політику. Цілком імовірно, вважають дослідники, що з початком війни російський державний апарат забажав встановити контроль над кіберпростором, беручи «к ногтю» навіть ті групи, які виступили на боці РФ, але виявляли надмірну самостійність. По-друге, заява Conti спровокувала внутрішній конфлікт, оскільки не сподобалась тим членам, які були етнічними українцями, або росіянам, що стали на бік України, або взагалі тих, хто бажав зберігати антивоєнну етику. Невдовзі один з цих членів зрадив групу, що й призвело до витоку внутрішньої переписки.

Але найголовніше — бренд став асоціюватися з російським урядом, і жертви здирництва почали боятись платити викупи, щоб самим не потрапити під санкції. Від кінця лютого на рахунки Conti майже перестали надходити платежі. На додачу Держдеп оголосив винагороду у $20 млн за відомості, які допомогли б знищити Conti.

Кіберзлочинні колективи нерідко вдаються до хитрощів, коли надто відоме угруповання оголошує про саморозпуск і за якийсь час спливає знову під іншими іменем. Проте Conti, як виявили розслідувані, влаштувала цілу виставу. Впродовж двох місяців вона займалася створенням або активізацією дочірніх груп, які почали виходити на сцену ще до того, як було оголошено про розпуск Conti, а також заводила своє керівництво в менші групи, поглинаючи їх.

Аби приховати той факт, що колектив вже розділився на менші утворення, було залишено ар'єргард, який імітував бурхливу діяльність: публікував раніше викрадені документи, вів кампанії на злочинних форумах і взагалі удавав міцний і сильний колектив, що нібито навіть мав плани розширення діяльності. Операція мусила завершитись певним гранд-фіналом, достойним репутації Conti; масована атака на Коста-Ріку могла здаватись останньою відчайдушною спробою злупити якісь гроші, проте насправді, як вважає AdvIntel, її метою було привернути увагу публіки, завдяки чому було можливо найправдоподібніше зобразити власну смерть. Зокрема, з внутрішньої переписки видно, що, попри гучні заяви, група зажадала викупу у розмірі менш за $1 млн, вочевидь не сподіваючись отримати і його.

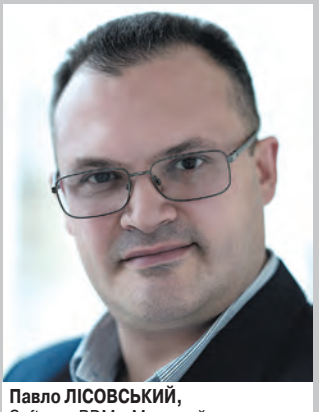
Здогадка про фіктивний саморозпуск Conti і продовження діяльності у формі інших груп підтверджується подальшими атаками. Відомо, що хакери, пов'язані з Conti, надалі беруть участь у кібервійні Кремля проти України. У липні дослідницька група IBM X-Force повідомляла, що така собі група ***ITG23***, відома також як ***TrickBot*** і під іншими іменами, від початку російського вторгнення систематично атакує Україну. Про подібні висновки писала на початку вересня дослідницька група ***Google Threat Analysis Group*** (TAG), яка досліджувала атаки з боку тієї самої групи, яку CERT-UA відстежує під іменем ***UAC-0098***.

До 24 лютого такі випадки ніколи не фіксувалися, і більшість їхнього зловмисного ПО було сконфігуроване так, щоб не запускатись при виявленні української мови. Проте з середини квітня по середину червня ITG23 здійснила принаймні шість кібератак, спрямованих проти українських органів влади, компаній та окремих громадян. Дослідники з AdvIntel зазначають, що сама група Conti свого часу виникла як частина TrickBot. Проте до кінця 2021 року Conti фактично викупила TrickBot, перетворивши його на свій підрозділ.

На основі багатьох ознак TAG робить висновок, що деякі з членів UAC-0098 є колишніми учасниками Conti, які переключилися на акції проти українських компаній і урядових структур, а також на європейські гуманітарні і неприбуткові організації. Зокрема, злочинці видавали себе за кіберполіцію і надсилали лінк нібито на оновлення операційної системи; в іншому випадку вони розсилали листи нібито з програмним забезпеченням Starlink. «*Діяльність UAC-0098 є прикладом розмиття межі між фінансово мотивованими і підтримуваними державою групами у Східній Європі, що ілюструє тренд, коли зловмисники обирають цілі з урахуванням регіональних геополітичних інтересів*», — йдеться у матеріалі TAG.

Fortinet звертає увагу на ще один приклад участі здирників у кібервійні. Дослідники FortiLabs виявили новий варіант здирницького ПО ***Chaos***, яке взагалі не надає ні засобу дешифрування, ні інструкцій, як зв'язатися зі здирниками — як видається, його призначенням є просто руйнування. Політичні повідомлення, які залишає шифрувальник, вказують на те, що хакери є проросійськими і що ситуація їх дратує. І позаяк війні не видно кінця, FortiGuard очікує появи іншого подібного ПО.

ЛОВИМО БОТІВ І ВІДБИВАЄМО DDoS-АТАКИ



Павло ЛІСОВСЬКИЙ,
Software BDM, «Мегатрейд»

У більшості веб-атак тим чи іншим чином задіяні шкідливі боти. Їх використовують для крадіжки контенту, витягування даних (data scraping) і особливо для DDoS-атак – останні, за інформацією компанії Reblaze (звіт 2022 State of Web Security Survey), у 2021 були найпоширенішим видом кіберзагроз: з ними зіткнулась половина респондентів. Тому точна ідентифікація ботів має вирішальне значення для надійної безпеки веб-інфраструктури.

При цьому сучасні боти досить-таки хитромудрі. Деякі з них дуже добре імітують людську поведінку. В результаті багатьом рішенням у галузі кібербезпеки складно відрізнити їх від людей. Дійсно, як свідчить опитування Reblaze, 50% компаній не знають, яка доля у їхньому трафіку припадає на шкідливих ботів, інша ж половина гадає, що знає, але насправді сильно недооцінює їхню кількість. Ці респонденти називають цифру у 6,2% трафіка, тоді як в реальності, згідно з підрахунками Statista, на них припадає 27,7% (до речі, на 2,1% більше порівняно з роком попереднім). За даними компанії LexisNexis, лише у першій половині 2021 року кількість кібератак, вчинених за допомогою ботів, зросла на 41% порівняно з аналогічним періодом 2020-го, тоді як число атак, ініційованих людьми, скоротилось на 29%.

Reblaze знає, про що говорить, адже їхня платформа безпеки Web Security Platform забезпечує як захист від DDoS на 3, 4 та 7 рівнях OSI, так і ідентифікацію ботів і захист сайтів від них, а також інші функції безпеки. Платформа працює за моделлю SaaS, інтегрована з AWS, MS Azure та Google Cloud Platform і поєднує в собі машинне навчання та адаптивне виявлення загроз.

Reblaze має на своєму рахунку успішні проєкти захисту від DDoS-атак. Зокрема, рішення захищає глобальну платіжну платформу Payoneer, якою наразі користуються тисячі корпорацій. За словами віце-президента з IT-операцій Payoneer Ярона Вайса, компанія піддається атакам щогодини. Замовника привабили вміння платформи ідентифікувати ботів, прозорість обробленого трафіку, незалежність від хмарної інфраструктури (що дозволяє переходити від однієї хмари до іншої) та віддалене адміністрування, яке здійснюється командою експертів.

Ще один проєкт було реалізовано для онлайн-аукціону eBay, теж значної цілі для веб-атак (175 млн користувачів і 1,1 млрд одночасно виставлених лотів). Тут Reblaze працює спільно з Google Cloud Armor, надаючи правила захисту, які автоматично оновлюються. Окрім того, за допомогою машинного навчання Reblaze проводить адаптацію при зміні середовища загроз. Виявивши атаку, Reblaze автоматично повідомляє Cloud Armor, який її відбиває. Таким чином Cloud Armor та Reblaze блокують усі атаки 3-го і 4-го рівнів та атаки 7-го (прикладного) рівня.

DDoS і гігантоманія

Ще одним видом кіберзлочинності, на який вплинула війна, є DDoS-атаки. Як відомо, нападу РФ передувала наперед підготована кампанія проти сайту Міноборони, порталу «Дія», а також банкоматів та мобільних за стосунків «Ощадбанку» та «Приватбанку». Її метою було посіяти паніку в суспільстві. Як зазначає ***Cloudflare*** у звіті за другий квартал, DDoS-атаки проти України й надалі мають на мету придушити поширення інформації: майже 80% припали на сектори мовлення, Інтернету, онлайн-ЗМІ і друкованої преси. З іншого боку, якщо на початку війни в росії найбільше зазнавали атак онлайн-медіа, то тепер 45% спрямовані на банки, фінансовий сектор і страхування. З обох сторін використовуються глобально рознесені бот-мережі.

Ендрю Фейбер, глава відділу веб-безпеки компанії ***Gcore***, в матеріалі на сайті Bleeping Computer зазначає, що якщо досі головними об'єктами атак були малі і середні компанії, то тепер усе частіше ними стають держустанови. На початку року було зафіксовано 10 чи не найпотужніших атак за останній час, і майже всі вони були спрямовані проти державних органів і підприємств; з них 5 — українських.

Водночас держави починають відігравати активну роль у боротьбі з DDoS-атаками. Наприклад, у лютому генеральний прокурор США публічно підтвердив, що ФБР провело секретну операцію зі знищення російського зловмисного ПО, чим запобігло масштабній кібератаці. З іншого боку, створена в Україні «Кіберармія» має завдання забезпечувати захист інформації і критичної інфраструктури. Таке активне втручання держави в індустрію цілком може назавжди фундаментально змінити ринок, пише пан Фейбер.

З технологічної точки зору трендом є зростання числа багатовекторних DDoS-атак — порівняно з минулим роком їх стало утричі більшим. Також, за даними Gcore, набувають поширення ультракороткі атаки — у 2022 році їх середня тривалість складала 5–10 секунд. Найдовша була зафіксована у квітні, вона відбувалась впродовж 24 годин і мала об'єм у 5 Гбіт/с. Середня потужність атак порівняно з минулим роком подвоїлась (700 проти 300 Гбіт/с).

Те, що DDoS-атаки стають дедалі потужними, підтверджує і Cloudflare. У другому кварталі кількість об'ємних атак величиною понад 100 Гбіт/с зросла на 8% проти попереднього кварталу. Впродовж минулого року компанія фіксувала рекордні атаки, одна сильніша за іншу. Вже у червні Cloudflare побороло DDoS-атаку потужністю у 26 млн запитів на секунду. Спричинила її маленька, але дуже потужна бот-мережа з 5067 пристроїв, кожен з яких на піку генерував близько 5200 запитів на секунду. Прикметно й те, що атака відбувалась через протокол HTTPS, а це дорожче порівняно з HTTP, бо вимагає більше обчислювальних ресурсів для створення шифрованого з'єднання; водночас і захищатися теж важче. Дослідники з'ясували, що атака йшла здебільшого не від Інтернет-провайдерів, а від постачальників хмарних послуг, тобто її генерували зламані віртуальні машини і потужні сервери, а не набагато слабші пристрої IoT.

Як зауважує компанія ***Imperva***, хоча атаки величиною у понад мільйон запитів на секунду не дивина, досі вони тривали від кількох секунд до лічених хвилин. Проте 27 червня Imperva відбила DDoS-атаку, яка тривала понад 4 години і на піку сягнула 3,9 млн запитів на секунду, при цьому компанія зауважує, що оскільки її рішення блокує атаки впродовж трьох секунд,

вона могла б сягнути набагато більших швидкостей. Об'єм атаки був узагалі рекордним: 25,3 млрд запитів загалом. Жертвою став китайський телекомунікаційний оператор. Зловмисники використали технологію мультиплексування, тобто об'єднання кількох пакетів в один, що дозволяє надсилати кілька запитів одразу. Бот-мережа налічувала понад 170 тис. IP-адрес у більш ніж 180 країнах (здебільшого в США, Індонезії та Бразилії), у тому числі використовувались маршрутизатори, камери відеоспостереження і скомпрометовані сервери. На деяких з тих серверів працювали публічні хмари або навіть провайдери послуг хмарної безпеки (Карл!).

Тим часом ***Akamai*** зафіксувала рекордні атаки проти цілей у Східній Європі: 659,6 млн пакетів на секунду у липні і 704,8 млн пакетів на секунду у вересні. І хоча за світовими мірками ті цифри не вражають, прикметно те, що під час вересневої атаки злочинці вдарили не лише по основному дата-центру компанії, а загалом по шістьох об'єктах у Європі та Північній Америці. Впродовж 60 секунд атака збільшилась зі 100 до 1813 активних IP на хвилину, причому ці адреси були рознесені по вісьмох підмережах у шістьох різних місцях планети.

Взагалі Akamai серед своїх клієнтів розрізняє «ультраризикових», тобто тих, кого DDoS-ять ледь не щодня (зокрема, один в середньому зазнає 3,1 атак на добу), і «нерегулярні цілі», у яких середній проміжок між серйозними атаками становить 106 діб. У 2017 році Akamai виділила 10% розташувань користувачів, які найчастіше зазнавали атак, але за наступні 5 років їхнє число більш ніж подвоїлось, сягнувши 26,1% (**рис. 3**). Це означає, що злочинці ширше розкидають свої сіті, прагнучи відшукати слабкі місця і вразливих жертв, що не мають належного захисту, і атакують не лише очевидні цілі, підключені до Інтернету, але й глибшу інфраструктуру, яку потрібно розвідувати.

Загроз багато, а людей мало

Якщо вести мову про інші виклики кібербезпеки, не пов'язані з війною в Україні, то їх теж чимало. Міжнародна консалтингова компанія ***McKinsey*** у березні оприлюднила три найважливіші, на її думку, тренди. Насамперед вона відзначає небезпеку, пов'язану з повсюдним доступом до даних. Нині, через поширення мобільних платформ і віддаленої роботи, невпинно зростає потреба у швидкісному і повсюдному доступі до даних, що підвищує ризик витоків. Аби краще розуміти поведінку споживачів і прогнозувати попит, організації збирають різноманітні дані — наприклад, про фінансові транзакції і перегляди сторінок у соцмережах. При цьому компанії не лише накопичують дані, але й централізують їх, зберігають у хмарах надають доступ різним

Рис 3. DDoS-атаки на нерегулярних цілей за останні 5 років (джерело: Akamai)

людям і організаціям, у тому числі постачальникам. Це вже призвело до низки гучних зламів — зокрема, у 2020 році відбулась відома атака Sanburst, у якій зловмисний код поширювався через рутинне оновлення ПО. Тоді ж через скомпрометовані облікові даних співробітника злочинці отримали доступ до інформації про 5,2 млн гостей готельної мережі Mariott.

Другою серйозною небезпекою є використання хакерами штучного інтелекту, машинного навчання та інших засобів автоматизації. Завдяки цьому цикл підготовки атаки скоротився з кількох тижнів до днів чи навіть годин, а також вдається видозмінювати засоби атак для збільшення їхньої ефективності. Наприклад, у 2020 троянець Emonet для створення таргетованих фітингових листів, зокрема на тему COVID-19.

Третьою проблемою McKinsey називає брак кадрів, знань і досвіду з кібербезпеки в багатьох організаціях. Загалом управління кіберризиками не встигає за темпами цифрової трансформації. Водночас регуляторні вимоги щодо захисту персональних даних стають усе жорсткішими, що є зокрема наслідком гучних витоків інформації і створює додаткове навантаження на відділи кібербезпеки.

Gartner у своїй оцінці основних кіберзагроз також звертає увагу на ризики, що виникли через поширення гібридного режиму роботи і міграцію до хмар. Наразі 60% інформаційних працівників виконують роботу віддалено, і щонайменше 18% не планують повертатися до офісів. Цей тектонічний зсув, а також повсюдне використання публічних хмар, ланцюжків постачання ПО і кіберфізичних систем (тобто загалом механізмів, що обладнані сенсорами і керуються комп'ютерами) — усе разом створило нові «поверхні атак» і зробило організації більш вразливими.

Gartner також характеризує нецільове використання облікових даних як основний метод, за допомогою якого злочинці проникають у комп'ютерні системи, а також на ризики, пов'язані з ланцюжками постачання ПО: за прогнозами агенції, до 2025 року 45% організації у всьому світі зіткнуться з атаками через постачальників — утричі більше, ніж у 2021-му.

Серед суттєвих трендів з боку кіберзахисту Gartner називає консолідацію виробниками функцій безпеки в єдиній платформі, що спрощує складність, скорочує вартість і збільшує ефективність захисту.

Іншим важливим трендом є поява архітектурного принципу «Сітка кібербезахисту» (Cybersecurity Mesh Architecture — CSMA). Її головними принципами є взаємосумісність і координація між різними продуктами, результатом чого є більш скоординована політика безпеки порівняно зі спробами захищати усі ресурси за допомогою однієї технології. CSMA адаптована до ситуації, коли організація не має єдиного фізичного периметра, і будь-який зовнішній вузол мережі може бути використаний злочинцями для проникнення в неї.

Зокрема, сітка кіберзахисту уможливлює безпечну інтеграцію у бізнес підприємства сторонніх програм і послуг, створення нових захищених каналів дистрибуції, а також безпечне розширення мережевої інфраструктури. Gartner прогнозує, що до 2024 року у організаціях, що впровадили CSMA, фінансові збитки від інцидентів кібербезпеки скоротяться на 90%.

Компанія ***Reblaze*** у своєму звіті 2022 State of Web Security Report, оприлюдненому на початку року, зазначає, що компанії активно впроваджують хмарні технології захисту: 64% респондентів вже використовують нативний екран веб-застосунків від свого хмарного провайдера (CSP WAF), адже його легко розгорнути й контролювати. Проте CSP WAF не захищає від усіх форм веб-атак, тому багато організацій продовжують використовувати інші технології: сторонні екрани або універсальні платформи, які поєднують WAF, анти-DDoS, контроль ботів, захист API тощо.

При цьому WAF залишається найпопулярнішим рішенням, яке компанії планують використовувати надалі: його назвали 60% респондентів; 31% вказали універсальні платформи, і 30% — мережу доставки контенту (CDN), що надається хмарним провайдером. Прикметно, що з-поміж великих відділів безпеки, які налічують від 6 і більше працівників, 40% збираються використовувати універсальні платформи порівняно з 24–34% серед менших відділів. Великі групи мають більше роботи, і їм зручніше працювати з пакетом, ніж з кількома точковими рішеннями. Водночас серед великих компаній зростає популярність виділених систем захисту від DDoS-атак.

Загалом понад дві третини опитаних компаній очікують, що їхні бюджети на веб-безпеку у поточному році зростуть, і лише 3% вважають, що вони зменшаться. В середньому зростання бюджету на веб-безпеку прогнозується на рівні 11,4% порівняно з 2021 роком.

З організаційної точки зору Gartner виділяє два тренди. По-перше, через цифровізацію багатьох аспектів бізнесу, управління кіберзахистом стає надто складним для єдиного директора з IT-безпеки (CISO). Тому провідні організації створюють «офіс CISO», який забезпечує децентралізоване прийняття рішень. Сам CISO продовжує надалі встановлювати політику безпеки, тоді як конкретні кроки визначаються на місцях.

Оскільки у більшості успішних хакерських атак присутній людський чинник, традиційні підходи до навчання персоналу правилам безпеки не надто працюють. Тому передові організації не обмежуються обов'язковим навчанням «для галочки», якого вимагають регуляторні документи, а запроваджують програми, спрямовані на зміну поведінки і культури праці.

Що до самих користувачів, то ось поради від Embroker: звести до мінімуму перенесення даних між робочими і особистими пристроями (що, втім, часто неминуче при віддаленому режимі роботи), не завантажувати зайвих файлів, тим паче з неперевірених джерел, використовувати паролі у вигляді беззмістовних рядків символів і ніколи їх не записувати, регулярно оновлювати ПЗ. Прості кроки, які рятують від непотрібних витрат.

Василь ТКАЧЕНКО, **МтБ**