IoT та його захист від кіберзагроз

Розумний холодильник може поцупити гроші.

Як і прогнозувалося, у світі лік пристроїв «Інтернету речей» (камери, датчики, точки доступу, медичні прилади, автомобілі тощо) пішов уже на мільярди. Ці пристрої зазвичай не мають достатньо пам'яті для встановлення захисних програм, їхні програми і паролі часто не оновлюються, тому вони вразливі для зламу. Найбільше на слуху бот-мережі з десятків тисяч зламаних домашніх маршрутизаторів і IP-камер, які вчиняють потужні DDoS-атаки, проте сценарії використання IoT у зловмисних цілях цим не обмежуються: підслуховування і крадіжка даних, фішинг, виведення з ладу обладнання, — ось чим загрожує злам IoT.

«МтБ» розбирався, яку ще небезпеку становлять незахищені IoT-пристрої та як, власне, їх захистити.

За два роки кількість атак потроїлась

IoT-пристрої численні і вразливі. Оскільки вони підключені до Інтернету або бездротових мереж, це дає змогу хакерам так чи інакше отримати до них доступ. При цьому пристрої є зазвичай слабо захищеними, оскільки не мають на борту достатньо обчислювальних ресурсів для роботи антивіруса та інших програм. Ці пристрої мають слабкі закладені паролі, які користувачі не міняють і часто навіть не знають, що це можливо, або ж оновлювати це ПЗ складно з технічних причин. Слабкий пароль робить ці пристрої вразливими для атак методом перебору (brute force). За оцінками Palo Alto Networks станом на 2020 рік, 57% пристроїв вразливі до атак середнього і високого рівня складності і часто самі постачаються з вбудованими вразливостями.

Якщо організація має велику кількість підключених пристроїв, вона може мати проблеми з їх відстеженням, контролем даних, які вони генерують, тим більше, що (за даними Palo Alto) 98% трафіку IoT-пристроїв не шифрується.

Важливим чинником стала прискорена цифрова трансформація, яка відбувалась останніми роками через пандемію COVID-19. Зокрема значно зросла кількість IP-камер, мережевих динаміків та маршрутизаторів, які використовувались для віддаленої роботи і навчання. Це все відбувалося зазвичай без належної уваги до кібербезпеки, що відкрило нові можливості для злочинців.

Check Point порахував, що у перші два місяці 2023 року середня кількість атак проти пристроїв IoT за тиждень в обрахунку на одну організацію зросла на 41% порівняно з 2022-м і утричі проти 2021-го. В середньому атак, цілями яких були IoT-пристрої, зазнали 54% організацій, а загалом на організацію в тиждень припадало в середньому 60 атак. Вони були спрямовані проти різноманітного обладнання: маршрутизаторів, IP-камер, цифрових відеореєстраторів, мережевих відеореєстраторів, принтерів та багато чого іншого.

Зростання числа атак зафіксовано у всіх секторах економіки, майже скрізь на двозначні величини, а у сфері освіти і науки взагалі відбувся безпрецедентний сплеск (**рис. 1**). Хакери атакують школи, бо вважають їх легкою здобиччю. У шкільних мережах містяться величезні обсяги персональних даних. Через перехід на віддалений режим до цих мереж підключилося безліч пристроїв IoT, які можна легко зламати, а коштів на кіберзахист бракує.

Статистику атак вже з використанням самих пристроїв IoT за типами публікувала ізраїльська компанія ***SAM***, яка спеціалізується на захисті автономних мереж і підключених пристроїв. Дані за 2021 рік і вочевидь дещо застаріли, але повинні бути

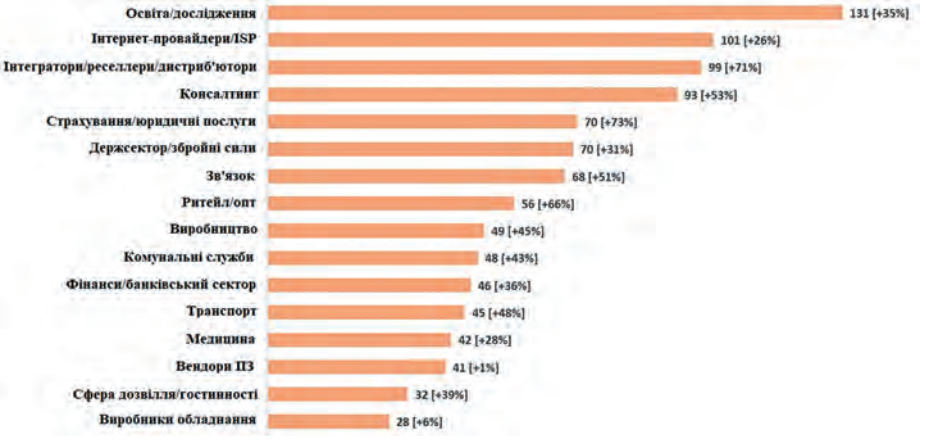

Рис. 1. Середня кількість атак проти IoT на тиждень в обрахунку на одну організацію у січні-лютому 2023 року і динаміка порівняно з 2022 роком. Джерело: Check Point

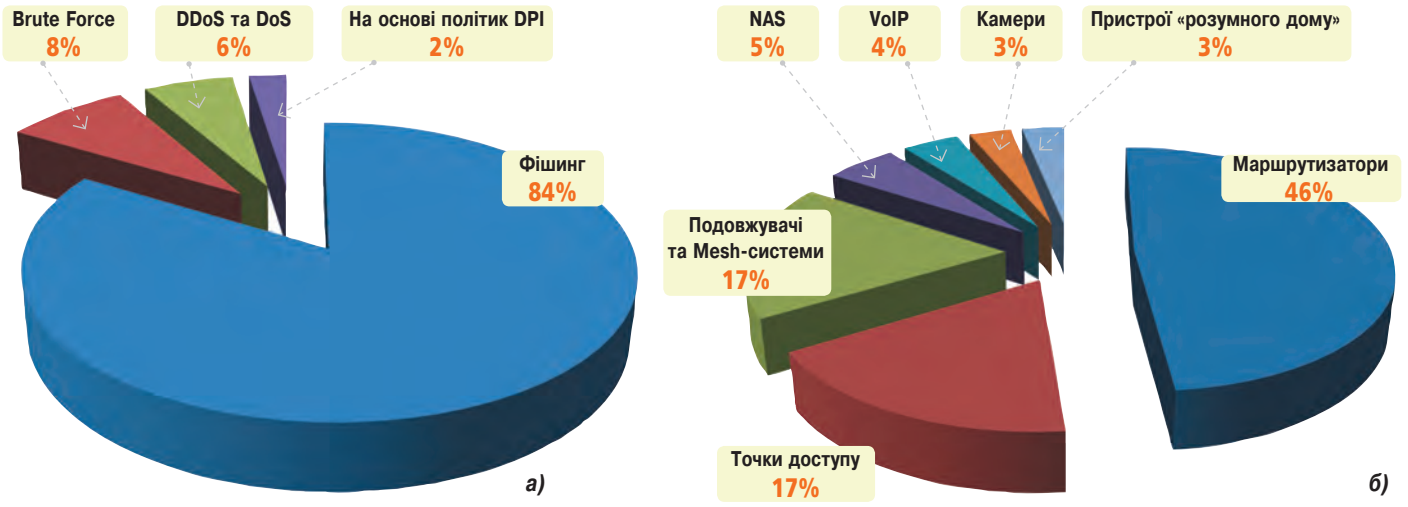

Рис. 2. Типи атак з використанням IoT (а) та найбільш вразливі категорії IoT-обладнання (б) у 2021 році. Джерело: SAM Seamless Network

все ще репрезентативними, тому що відображають момент, коли всі вже перелаштувалися на гібридний і віддалений режими роботи. Отже, проаналізувавши дані з 132 млн активних IoT-пристроїв і 730 тис. мереж, SAM зафіксувала протягом року понад 1 млрд атак, абсолютна більшість з яких була фішинговими (**рис. 2а**).

IoT-пристрої використовувались у наймасовіших на той момент DDoS-атаках. Проти компанії Cloudflare «працювали» понад 20 тис. ботів, скомпрометованих за допомогою ПЗ сімейства Mirai, які надіслали понад 330 млн запитів. Самі боти розташовувались у 125 країнах, переважно в Індії, Індонезії та Бразилії. Інші атака, яка вразила російську компанію Yandex і американський блог з кібербезпеки KrebsOnSecurity, налічувала 250 тис. скомпрометованих мережевих пристроїв Mikrotik.

Загалом найбільш вразливими до атак IoT-пристроями є маршрутизатори, точки доступу та інше обладнання бездротових мереж (**рис. 2б**). Причина проста: переважна більшість домогосподарств та бізнесів мають принаймні один такий. Найчастіше це обладнання є вразливим до атак через те, що користувачі не змінюють паролі, не оновлюють ПЗ і не застосовують сегментацію мережі.

Холодильники-зомбі і безпорадні замки

То, власне, як ламають пристрої IoT? Мабуть, чи не найвідоміший атакувальний код Mirai, який уперше проявився у 2016 році і генерував потужні DDoS-атаки (і який у різних варіантах існує донині), просто захоплював маршрутизатори й IP-камери, у яких не були змінені заводські імена і паролі. Злочинці мають словники таких базових комбінацій і застосовують їх для отримання доступу до пристроїв.

Поширений прийом — атака типу «людина посередині» (Man-in-the Middle — MitM). Він часто використовується у сценаріях підміни легітимної точки доступу чужою (Rogue AP), проте таким чином хакер може вклинитись і у з'єднання між домашніми або офісними пристроями. Як зазначає SAM, використовуючи спуфінг протоколу визначення адрес ARP, хакер може, наприклад, підмінити адресу принтера адресою маршрутизатора (**рис. 3**), у цьому разі принтер попереджатиме хакера, наприклад, про встановлення сеансу зв'язку з банком або іншою адресою, куди може бути відправлено цікаву інформацію. Хакнутий пристрій може використовуватись і для стеження за клієнтами компанії.

Зараз у світі дослідники вигадують сценарії зловживання IoT у превентивних цілях. В Інтернеті можна зустріти чимало прикладів таких експериментів. Зокрема, ламали біометричний висячий замок Tapplock, перехопивши його незашифрований потік даних по протоколу Bluetooth Low Energy (BLE) і визначивши його MAC-адресу, тоді як, підключившись до дверного дзвінка, вдалося отримати пароль до мережі Wi-Fi.

Є цікава стаття за авторством дослідників Раяна Хартфілда і Даян Ган, які розглядають різні сценарії

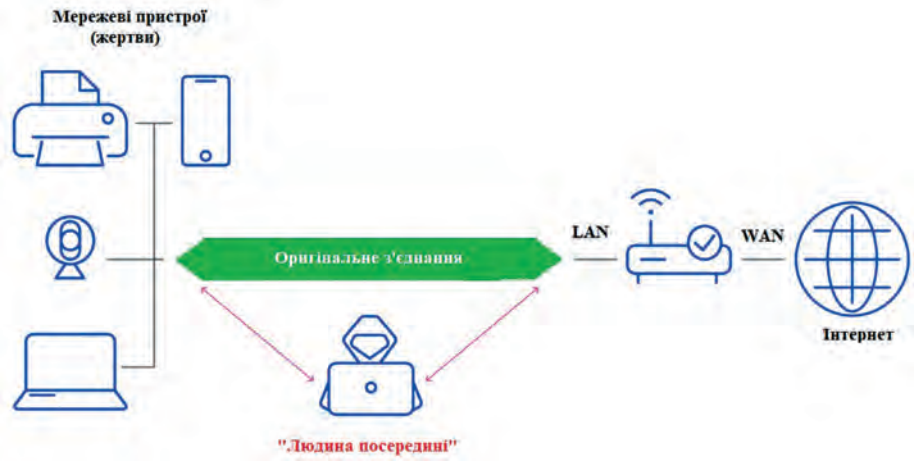

Рис. 3. Схема атаки типу MitM проти IoT. Джерело: SAM Seamless Network

використання скомпрометованих пристроїв IoT для фішингу. В одному з них хакери відстежують обмін даними між розумним холодильником і домашнім контролером, після чого відправляють користувачеві підроблене повідомлення, що нібито закінчилося молоко, з пропозицією купити його онлайн (за посиланням, звісно, завантажиться шкідливий код). До фішингових повідомлень, які надходять на електронну пошту, всі вже за кілька десятиліть звикли, зазначають автори, але що загрозу можуть становити прилади домашньої автоматизації, розумні пристрої або платформи е-медицини, публічних сервісів тощо, — цього ще користувачі не навчились розрізняти. (Конкретно атаки через холодильник реально мали місце — одна з найперших сталася у 2013 році, коли компанія Proofpoint виявила ботмережу з понад 100 тис. холодильників, розумних телевізорів та інших побутових приладів, які розсилали спам).

Перевіряй і не довіряй

Правила захисту IoT не такі вже й складні. Експерти і компанії в галузі кібербезпеки (вендори, провайдери послуг) пропонують більш-менш подібний набір рекомендацій.

Зокрема, вони радять використовувати систему контролю доступу до мережі (***NAC***) — категорію продуктів безпеки, яка поєднує технології захисту кінцевих точок з механізмами автентифікації користувачів і забезпечення мережевих політик. NAC надає доступ до мережі на основі політик безпеки, ролей і власної захищеності пристроїв. У даному разі NAC допоможе ідентифікувати і обліковувати пристрої IoT, як підключаються до мережі, і відстежувати їх.

Корисно запровадити модель нульової довіри (***Zero Trust***), яка взагалі передбачає верифікацію і авторизацію всіх користувачів незалежно від того, знаходяться вони в мережі організації чи поза нею, а також постійне оцінювання їхньої конфігурації безпеки перед наданням доступу до програм і даних. Додатковий рівень захисту — як корпоративним, так і побутовим користувачам, — забезпечить багатофактора автентифікація при доступі до пристроїв та мереж.

Варто реалізувати сегментацію, тобто виокремити IoT-обладнання, яке потребує підключення до Інтернету, в окрему підмережу з обмеженим виходом на загальну корпоративну мережу. Надалі у цьому внутрішньому сегменті можна відстежувати аномальну активність. Для автоматизації сканування пристроїв і управління ними стануть у нагоді алгоритми машинного навчання, які можуть автоматично зупиняти атаки, сповіщаючи IT-персонал постфактум.

Критично важливо забезпечувати своєчасне оновлення ПЗ і самих пристроїв, мати якусь систему управління вразливостями і наперед задумуватися про термін служби пристроїв. Потрібне навчання співробітників, відповідальних за кібербезпеку, які повинні вчасно освоювати нові та незнайомі системи і бути готовими до нових викликів. Зі свого боку, кінцеві користувачі теж повинні бути в курсі небезпеки, яку становлять IoT-системи, і самим вживати заходів для їх убезпечення (змінювати заводські паролі і регулярно завантажувати оновлення). Окрім того, споживач може чинити тиск на виробників, не купуючи обладнання, яке не відповідає стандартам безпеки.

Виробники рішень у сфері кібербезпеки мають свої продукти для захисту IoT, які забезпечують профілювання пристроїв, їх контроль і моніторинг, автоматизоване генерування і впровадження політик доступу Zero Trust, реагування і сповіщення. Для цього вони співпрацюють з виробниками IoT і використовують дані, зібрані власними аналітичними службами.

Наприклад, ***Fortinet*** може запропонувати лінійку контролерів доступу FortiNAC з підтримкою Zero Trust. Це рішення забезпечує мікросегментацію мережі, сканування та ідентифікацію підключеного обладнання (може класифікувати 71 тис. унікальних пристроїв від понад 150 виробників, підтримує 72 мережеві протоколи). Система реагує на події безпеки і надсилає сповіщення адміністратору. Для підключених пристроїв забезпечується доступ з мінімальними привілеями, а також реавтентифікація і безперервний моніторинг. Як і загалом продукти Fortinet, FortiNAC інтегрується з іншими рішеннями архітектури Security Fabric для забезпечення ще кращої видимості, реагування і управління політиками.

Palo Alto у своїй стратегії виходить з того, що існуючі класи рішень не надто підходять для IoT. Сканери вразливостей — через велике розмаїття пристроїв, NAC — через обмежені можливості і масштабованість, а спеціалізовані системи вимагають надмірних зусиль в адмініструванні. Тому компанія пропонує для захисту IoT рішення Enterprise IoT Security, доступне у вигляді хмарної підписки для мережевих екранів (NGFW). Рішення вміє ідентифікувати підключені пристрої, використовуючи власну технологію App-ID, трирівневу модель машинного навчання і краудсорсингову телеметрію, що дозволяє класифікувати обладнання загалом за 50 атрибутами. Функції NGFW забезпечують захист від атак, а загрожені пристрої автоматично ізолюються від мережі, даючи час персоналу для вжиття заходів. Порівнюючи поведінку пристроїв з краудфандинговими даними, система автоматично виробляє рекомендовану політику доступу для них.

У ***Check Point*** рішення Quantum IoT Protect також інтегроване у мережеві екрани Quantum Security Gateways і забезпечує багатошаровий захист пристроїв, у тому числі від атак нульового дня. Рішення розпізнає і контролює понад 1500 протоколів IoT/OT, має понад 300 готових сигнатур для розпізнавання атак. Виробникам IoT компанія пропонує пакет Quantum IoT Protect Firmware, за допомогою якого можна оцінити вразливості пристрою і вбудувати програму Quantum IoT Protect Nano Agent, щоб з її допомогою захищати пристрої від відомих та невідомих атак. Пристрої з «наноагентом» на борту можна контролювати через хмарний портал.

Загрози IoT і захист від них дедалі більше перетворюються на проблему, переходячи з області кіберпанку в повсякденне життя. Боротьба снаряда та броні триває.

Василь ТКАЧЕНКО, **МтБ**