doi: <https://doi.org/10.15407/emodel.41.06.091>
УДК 519.7-004.65

М.Ю. Комаров, аспірант

Інститут проблем моделювання в енергетиці ім. Г.Є.Пухова НАН України
(Україна, 30164, Київ, вул. Генерала Наумова, 15,
тел. (+38) 098 7000344, e-mail: maxkom@i.ua)

Огляд кібератак на об'єкти критичної інфраструктури

Подано аналітичний огляд найвідоміших кібератак на об'єкти критичної інфраструктури. Наведено прогноз актуальних кіберзагроз на 2020 рік.

Ключові слова: кібербезпека, кібератака, уразливість, комп'ютерний вірус, захист мережі.

Дослідження кібернетичної захищеності об'єктів критичних інфраструктур завжди пов'язано з аналізом інцидентів, що дозволяє виявити неявні закономірності та системні проблеми. Саме тому спеціалістам з кібернетичної безпеки потрібно знати про найбільш резонансні кібератаки, які призвели до значних економічних втрат або загибелі людей, а також передумови, що їх спричинили, та наслідки їх реалізації. Особливу увагу приділимо аналізу фактів, що сприяли імплементації атак.

Історія найнебезпечніших кібератак. Сибірський нафтопровід.

Зазвичай всі сучасні кібератаки здійснюються через мережу Інтернет. Але перша кібератака сталася ще до появи Інтернету – в 1982 році. Тоді група хакерів змогла встановити троян в SCADA-систему, яка контролювала роботу сибірського нафтопроводу, що призвело до потужного вибуху. Атака була організована ЦРУ, хоча про це не було відомо до 2004 року, коли секретар Міністерства оборони США і радник президента Рейгана Томас Рід опублікував свою книгу [1].

Даний інцидент став першим «дзвоником», що пролунав як попередження на фоні стрімкого розвитку індустріальних систем та об'єктів критичної інфраструктури. Відтепер стало зрозуміло, що для виведення з ладу критично важливих об'єктів або заподіяння шкоди таким об'єктам зовсім

© Комаров М.Ю., 2019

не обов'язково реалізовувати цілеспрямований фізичний вплив, такий як диверсія, підриг, атака із застосуванням класичних видів озброєння. Група молодих людей, «озброєних» знаннями в області функціонування об'єктів критичної інфраструктури, знаючи принципи кодування автоматизованих систем управління технологічними процесами та персональними комп'ютерами, здатна завдати більш руйнівного впливу, ніж спеціально навчений диверсійний підрозділ спеціального призначення.

Chevron. Наступний інцидент стався через десять років. У 1992 році було звільнено робочого нафтової компанії Chevron, який зламав комп'ютери в офісах компанії у Нью-Йорку і Сан-Хосе, що відповідали за системи попереджень. Зловмисник переналаштував їх на аварію після запуску системи. Ця атака не була розкрита, доки не сталося витіку отруйної речовини в Редмонді (штат Каліфорнія), при цьому система не видала відповідних попереджень. В результаті тисячі людей піддавалися значному ризику протягом 10 годин до відключення системи.

Цей випадок спонукав спеціалістів звернути увагу на такий аспект кіберзлочинності, як мотивація кіберзлочинця. Навіть така тривіальна причина, як образа за звільнення, може стати підставою для заподіяння шкоди установі, що позбулася небажаного працівника. При цьому об'єктивні або суб'єктивні причини не мають значення.

Salt River Project. У серпні 1994 року Лейн Джаррет Девіс зламав мережу Salt River Project, отримавши доступ до інформації і видаливши файли з системи, що відповідає за моніторинг і подачу води і електрики. Особливість цього випадку полягає в тому, що зловмисник вперше зумів отримати доступ до персональних і фінансових даних клієнтів і співробітників компанії. Недостатня увага щодо захисту персональних даних зробила можливою цю кібератаку. Наразі суспільство прийшло до розуміння необхідності захисту персональних даних як фундаментального права фізичної особи, що є основою та підґрунтям загальних прав людини [2].

Aeronopm Worcester. Інші ключові сектори критичної інфраструктури також піддавалися спрямованим атакам. 10 березня 1997 року хакер проник у систему управління, яка використовується для комунікацій системи контролю повітряного руху в Вустері (США, штат Массачусетс), викликавши збій системи, що спричинило відключення телефонного зв'язку на шість годин. Особливо це вплинуло на телефонну систему вежі управління пожежної служби аеропорту і авіакомпаній, що базуються в аеропорту. Попри те що на той час вже були відомі факти кібератак на мережі телефонного зв'язку, однак вперше впливу піддалася службова мережа.

Фахівці з безпеки констатували, що мережі службового телефонного зв'язку тепер є черговим об'єктом потенційних кібератак та потребують такого ж ретельного захисту, як і комп'ютерні мережі.

Maroochy Water System. Колишній співробітник компанії Maroochy Water System (Австралія) отримав два роки тюремного ув'язнення за злам у 2000 році системи управління водопостачанням. В результаті цієї атаки мільйони літрів стічних вод потрапили в найближчу річку, що, крім екологічного лиха, призвело до затоплення місцевого готелю.

Сумнозвісний людський фактор — наразі це найменш прогнозований, а тому найбільш загрозливий чинник реалізації кіберзагроз на будь-які мережі та системи.

Газопереробний завод, побудований американською компанією, також піддався атаці в 2001 році. Шість місяців тривало розслідування, в результаті якого встановлено, що атаку було здійснено одним з постачальників, який для приховування зробленої ним помилки, вирішив відвернути увагу, зламавши три персональних комп'ютери компанії, тим самим викликавши відключення подачі газу для домашніх і корпоративних клієнтів в одній з європейських країн. Компанія-постачальник природного газу вирішила, що її репутаційні втрати від розголошення фактів власної некомпетентності значно перевищать витрати на організацію кібератаки. В результаті окрім витрат на здійснення кіберзлочину компанія понесла репутаційні втрати, до яких, окрім втрат від некомпетентності, додалися репутаційні втрати від причетності до кібератаки (а фактично від її реалізації).

PDVSA. У грудні 2002 року нафтова компанія PDVSA з Венесуели піддалася атаці, в результаті якої видобуток нафти скоротився від 3 млн. до 370 тис. барелів на добу. Під час атаки було зламано кілька корпоративних комп'ютерів. Атаку здійснено під час страйку працівників підприємства для того, щоб скерувати на них підозру.

Економічні та соціальні вимоги не рідко стають рушійною силою здійснення кібератак.

Світлофори в Лос-Анджелесі. У 2006 році два інженери з організації дорожнього руху в Лос-Анджелесі зламали міські світлофори в знак протесту. Їм вдалося змінити програму роботи деяких світлофорів, розміщених на важливих ділянках, після чого вони стали горіти червоним світлом, що призвело до серйозних пробок.

Вмотивований фахівець високого класу, причетний до створення інформаційної системи, — небезпечна зброя, здатна нанести непоправну шкоду, особливо тим об'єктам, до створення та впровадження яких він був причетний.

Трамвайна мережа в Лодзі. У 2008 році 14-річний студент зламав системи трамвайної мережі в польському місті Лодзь. В результаті атаки чотири трамвая зійшли з колії, а 12 осіб отримали травми. Студент створив інфрачервоний пульт дистанційного керування, за допомогою якого він зміг контролювати трамвайні перехрестя.

Потяг до самореалізації та самоствердження, особливо у молодих людей, здатен штовхати їх до різноманітних безглуздих, а в деяких випадках і небезпечних вчинків. Спрямування таланту та енергії у конструктивне русло — завдання, що лежить в стратегічній площині забезпечення кіберзахисту об'єктів критичної інфраструктури.

Saudi Aramco. У 2012 році найбільша нафтова компанія в світі Saudi Aramco стала жертвою атаки, спрямованої на її офіси. Хакери отримали доступ до мережі завдяки атаці на одного зі співробітників компанії, через якого змогли отримати доступ до 30 000 комп'ютерів в мережі. У певний момент хакерам вдалося видалити вміст всіх комп'ютерів тоді, як на екранах показували палаючий американський прапор. Відповідальність за атаку взяла на себе група хакерів, які називали себе «Меч правосуддя».

Соціальна інженерія останнім часом заявляє про себе як про один з найрозповсюдженіших інструментів реалізації кібератак. Коли технічний захист інформаційних систем набув достатньо високого рівня, слабкі місця кіберзлочинці почали шукати через людей. Емоції — це те, що відрізняє нас від комп'ютера. Саме цей «фактор» все частіше використовують кіберзлочинці.

Ram Gas. Через два тижні після атаки на Saudi Aramco катарську компанію RamGas — другого в світі виробника скрапленого природного газу, було атаковано тією ж шкідливою програмою, яку використано для атаки на нафтову компанію Саудівської Аравії. Протягом декількох днів не працювали внутрішня корпоративна мережа і веб-сайт компанії.

Металургійний завод в Німеччині. У 2014 році в Німеччині жертвою атаки став один з металургійних заводів. Використовуючи соціальну інженерію, хакери змогли отримати доступ до комп'ютера одного співробітника, а з його комп'ютера вони отримали доступ до внутрішньої мережі системи управління. В результаті цього стало неможливим вимкнути один з доменів, що завдало великої шкоди підприємству.

Захват комп'ютерної мережі підприємства відбувався у два етапи. Спочатку хакери взяли під свій контроль електронну пошту працівників заводу, розіславши їм листи з фітінговими посиланнями. Через пошту співробітників хакери отримали доступ до офісної мережі підприємства, а потім — до системи, яка керувала доменними печами.

Як зазначають фахівці з кібербезпеки, найімовірніше замовниками цього нападу є великі злочинні угруповання, або навіть держави, які задля досягнення конкурентної переваги на міжнародних ринках не хestують такими брудними методами.

Електромережа України. Наприкінці 2015 року Україна зазнала кібератаки на національну електромережу, в результаті чого понад 600 000 жителів залишилися без електрики.

Так звана гібридна війна, яку веде країна-агресор проти України, триває і в інформаційному просторі. Кібератаки на об'єкти критичної інфраструктури, які спостерігаються в останні роки, за своїм руйнівним потенціалом можна вважати зброєю масового ураження. Вочевидь, одним з основних напрямків оборонної стратегії держави має стати захист державних інформаційних ресурсів та систем від кіберзагроз та кібератак з боку інших держав та міжнародних злочинних хакерських угруповань.

Перша в історії кібератака проти Інтернет-інфраструктури. Незважаючи на довгий список інцидентів, перша в історії кібератака на Інтернет-інфраструктуру сталася 27 квітня 2007 року, коли в Естонії ряд атак обрушив сайти різних організацій, включаючи парламент, різні міністерства, банки та ЗМІ. Атака була також спрямована на певні непублічні адреси, включаючи національну систему обробки фінансових ордерів і телекомунікаційні служби. Міністр закордонних справ Естонії публічно звинуватив російську владу в причетності до даних атак.

Найвідоміший випадок кібератаки на критичну інфраструктуру: Stuxnet. У 2008 році людство стало свідком одного з найбільш сумно відомих в історії випадків кібератак на критичні інфраструктури: Stuxnet. Зараз вже відомо, що це була скоординована атака ізраїльських і американських спецслужб, спрямована на зрив ядерної програми Ірану.

Спецслужби створили хробака, який заразив комп'ютери, що керують урановими центрифугами на іранському заводі в Натанзі, в результаті чого вони стали працювати на повній швидкості, водночас інженери на своїх моніторах спостерігали нормальний режим роботи. Це завдало фізичного збитку всім урановим центрифугам на заводі. Після цього випадку громадськість дізналася про подібні загрози.

Інші атаки на об'єкти критичної інфраструктури. Крім атак, спеціально здійснюваних для заподіяння шкоди критичній інфраструктурі, інші атаки, з якими стикаються компанії, також негативно впливають на критичні об'єкти, а їх наслідки іноді бувають такими ж серйозними.

Подібні проблеми почалися в кінці минулого десятиліття, тому що мережеві хробаки стали поширюватися в мережі самостійно. Наприклад,

в США на провідній фабриці з випуску продуктів харчування вірусна інфекція завдала шкоди, яка вимірюється тисячами доларів. Один співробітник віддалено підключився з домашнього комп'ютера, який був заражений вірусом Nimda. Як тільки він увійшов в корпоративну мережу, хробак поширився на всі системи управління.

У 2003 році нафтова компанія в США постраждала від хробака SQLSlammer, який проник у внутрішню мережу. Це не призвело до зупинки виробництва, проте він вплинув на внутрішні комунікації. Довелося витратити кілька днів для повного видалення хробака з мережі і оновлення систем для запобігання подальших атак.

Даний хробак був одним з найбільш руйнівних. Для поширення він використовував уразливість в серверах баз даних SQL (стандартний інструмент в корпоративних мережах). Уразливість була виправлена Microsoft у січні 2003 року. Інша американська нафтова компанія почала оновлювати всі свої об'єкти одразу ж після появи цього виправлення (патча), щоб захистити себе від хробака. Однак для завершення оновлення необхідно було перезавантажити сервери, на яких цей патч було встановлено. Деякі з них перебували на нафтових платформах, де не було спеціального ІТ-персоналу. Тому довелося відправляти фахівців на вертольоті, але до того як вони приїхали, хробак проник до деяких корпоративних систем і заразив ті з них, які ще не встигли оновити.

У тому ж 2003 році один з найбільших автовиробників США також постраждав від атаки хробака SQLSlammer, який миттєво поширився на його 17 заводах. Загальний збиток для компанії склав 150 млн. доларів США. Хоча патч вже був доступний протягом шести місяців, ІТ-менеджери компанії досі не встановили його.

У тому ж році від шкідливої інфекції (шкідлива програма не була публічною) постраждав комп'ютер авіакомпанії Air Canada, що відповідає за льотну інформацію, заправку палива та ін. В результаті інфекції 200 рейсів було затримано або скасовано.

У 2005 році в Японії комп'ютер співробітника компанії Mitsubishi Electric був заражений шкідливою програмою, що призвело до витоку конфіденційних інспекційних документів про дві атомні електростанції, які належать даній компанії.

У 2006 році два комп'ютери в лікарні (Великобританія), які відповідають за управління комплексом променевої терапії для хворих на рак людей, були заражені шкідливою програмою. В результаті довелося відкласти лікування 80 пацієнтів. Через два роки ще три лікарні у Великобританії було заражено варіантом хробака Mytob, після чого довелося

відключити всі комп'ютери від мережі на 24 години для розслідування інциденту.

У 2013 році було заражено 200 комп'ютерів Департаменту автомобільних доріг і транспорту в окрузі Кук (штат Іллінойс, США). Ці системи відповідали за підтримку сотні кілометрів доріг у передмісті Чикаго. В результаті атаки довелося відключати мережу на дев'ять днів, щоб відновити працездатність всіх комп'ютерів.

Цей список інцидентів показує, що небезпека кібератак на об'єкти критичної інфраструктури цілком реальна, і з розвитком інформаційних технологій ризику щодо їх здійснення збільшуються.

Додатковий захист критичної інфраструктури. На даний час актуальною є задача регулювання захисту критичної інфраструктури для забезпечення більш високого рівня захисту від усіх типів загроз [3].

У травні 2016 року після зустрічі міністрів енергетики країн G7 була прийнята спільна декларація, в якій серед іншого задекларовано важливість створення відмовостійких енергосистем (включаючи газ, електрику і нафту) для ефективного реагування на кіберзагрози і підтримання нормальної роботи життєво необхідних служб.

Для удосконалення заходів щодо запобігання і реагування на логічні атаки уряди країн здійснюють ряд заходів на глобальному рівні, які спрямовано на створення центрів зі збору всієї необхідної інформації. В результаті розроблено комплексну стратегію для вирішення даної проблеми, яка повинна бути включена в національне законодавство цих країн.

Захист від відомих атак повинен містити наступні заходи:

1. Перевірка систем на уразливість, особливо вже відомих.
2. Адекватний моніторинг мереж, які використовуються для контролю об'єктів критичної інфраструктури, і при необхідності їх повна ізоляція від зовнішніх з'єднань, що дозволить виявляти зовнішні атаки і запобігати доступу до систем, керованих з внутрішньої мережі.
3. Контроль над знімними пристроями, що важливо в будь-якій інфраструктурі не тільки тому, що вони є об'єктами таких атак, як у випадку з Stuxnet. При захисті таких об'єктів критичної інфраструктури вкрай важливо, щоб шкідливі програми не проникали у внутрішню мережу через знімні пристрої, які також можуть бути використані для крадіжки конфіденційної інформації.

4. Моніторинг ПК, до яких підключені програмовані логічні контролери (або PLC). Ці підключені до Інтернету пристрої є найбільш чутливими, тому що вони можуть надавати хакерам доступ до критично важливих систем управління. Навіть якщо вони не зможуть отримати конт-

роль над системою, вони зможуть отримати цінну інформацію для інших напрямків атаки.

Кіберзагрози, реалізовані у 2018 році. Перехоплення трафіку через вразливості Інтернет-маршрутизації BGP. Останнім часом почастішали випадки використання вразливостей в протоколі BGP. Перехоплення та перенаправлення трафіку дозволяє аналізувати його та маніпулювати ним, що призводить до крадіжок криптовалюти, порушення конфіденційності, встановлення контролю над комп'ютерами.

Восени 2018 року зафіксовано нову схему, що використовується злоумисниками для шахрайства з Інтернет-рекламою. Операція злоумисників, названа 3ve, дозволила перехопити трафік більш ніж 1,5 млн IP-адрес та змусити рекламні компанії повірити, що мільярди показів Інтернет-банерів дійсно було переглянуто реальними користувачами. В результаті цієї атаки рекламні компанії понесли збитки на суму приблизно 29 млн доларів, що було виплачено шахраям, які використовували вразливості та некоректне налаштування BGP.

Рекомендацією щодо запобігання даної загрози може бути коректне налаштування мережевого обладнання, а також моніторинг маршрутної інформації мережі за допомогою відповідних сервісів моніторингу BGP.

Злам мережевих пристроїв. В кінці листопада 2018 року виявлено 45 000 скомпрометованих маршрутизаторів. Ботнет із 100 000 скомпрометованих мережевих пристроїв (Broadcom, Asus, TP-Link, Zyxel, D-Link та ін.) було виявлено трохи раніше. У травні 2018 року фахівці Cisco Talos виявили півмільйона скомпрометованих мережевих пристроїв в 54 країнах світу. Серед потерпілих — компанії Asus, D-Link, Huawei, UPVEL, ZTE та ін. Злам мережевого обладнання стає дедалі масовішим явищем, позаяк дозволяє злоумисникам отримати доступ до великих обсягів інформації, що їх цікавить, та може передаватися у незашифрованому вигляді.

Як запобіжні заходи виробниками мережевого обладнання розробляються відповідні рекомендації з налаштувань, а також впроваджуються механізми безпечного завантаження, захист пам'яті, захист від підміни апаратних компонентів тощо. Крім того, доброю практикою буде аналіз телеметрії, яка надходить від мережевого обладнання, що дозволить ідентифікувати аномалії у мережевому трафіку та своєчасно виявити компрометацію на рівні мережевої інфраструктури.

Атаки на ланцюг поставок. У 2018 році Міністерство національної безпеки США повідомило про атаку невідомими хакерами енергетичних компаній у Північній Америці. Вплив відбувався за допомогою відомої атаки Waterhole, суть якої полягає у тому, що злоумисники починають

перший крок атаки не зі зламу компанії-жертви, а з компрометації сайту виробника програмного забезпечення (ПЗ) або обладнання, яке використовує жертва. Зрештою компанія приходить на сайт виробника за оновленнями ПЗ і прошивок та завантажує з довіреного ресурсу заражене ПЗ, цілком довіряючи йому. Так зловмисники потрапляють всередину організації та починають розширення плацдарму. Дана атака дозволяє заразити не одну, а одразу багато компаній, які мов до водопою (звідси назва Waterhole), приходять на сайт виробника за оновленнями.

В кінці серпня 2018 року авіакомпанія British Airways зіткнулася з тим, що декілька сотен тисяч її клієнтів постраждало від витоку даних платіжних карт, які вводилися на сайті при купівлі квитків. В процесі розслідування з'ясувалося, що хакерське угруповання Magecart зламало сайт підрядника British Airways, з якого і завантажувався заражений JavaScript, що спричинив виток інформації. Аналогічно діяло Magecart при атаках на сайт з продажу квитків Ticketmaster, а також інших ресурсів електронної комерції. Врешті решт, за однією з версій, постраждав не основний сайт British Airways, а один з його клонів, розміщених у CDN-інфраструктурі Інтернет-провайдера і призначених для прискорення доступу до сайту авіакомпанії з певних місць знаходження. У цьому випадку зламу піддався не сайт самої компанії, а один з її контрагентів, який надає частину своєї інфраструктури.

Ці приклади, а також наведений вище випадок з крадіжкою криптовалюти при перехопленні трафіку через BGP є свідченням того, що атаці можуть піддаватися не тільки ресурси компанії, що цікавлять хакерів, але і інфраструктури, що її обслуговують. За прогнозами спеціалістів такі атаки у майбутньому будуть частішати, що свідчить про необхідність розширення сфери уваги фахівців з кібербезпеки та розробки стратегії не тільки власної безпеки, але й контролю безпеки своїх партнерів, підрядників та контрагентів.

Універсального засобу запобігання даній загрозі немає. Все значною мірою залежить від того, як і яку інфраструктуру підрядника зламують зловмисники. Якщо це атаки на BGP, то необхідно здійснювати моніторинг BGP-маршрутів, якщо це атака через заражений скрипт на сайті скомпрометованого виробника, то допоможе моніторинг DNS (Domain Name System). Якщо йдеться про завантаження підміненої прошивки ПЗ, то може допомогти аналіз аномалій у телеметрії. Зрештою необхідно визнати, що дана загроза є досить актуальною та залишатиметься такою у 2020 році.

Вразливості протоколу TLS 1.3. В серпні 2018 року опубліковано рекомендацію RFC 8446, яка визначила нову версію TLS 1.3, до переваг якої можна віднести більш високу швидкість та криптографічну стійкість. При цьому усунуто вразливості попередньої версії і додано нові корисні функції.

На даний час TLS 1.3 підтримують багато популярних браузерів та криптобібліотек (наприклад, Chrome, Firefox, OpenSSL). Затримку у прийнятті TLS 1.3 було пов'язано, окрім іншого, з тим, що ця версія протоколу не дозволяє інспектувати трафік за допомогою проміжних пристроїв (NGFW, IDS, проксі та ін.), що необхідно для багатьох корпоративних служб кібербезпеки. Ряд компаній у процесі обговорення TLS 1.3 запропонували включити до нього більш слабкий протокол обміну ключами, але ці пропозиції було відхилено з метою забезпечення конфіденційності в Інтернеті та захисту від втручання держави у свободу комунікацій. При активному використанні TLS 1.3 неможливість його інспекції стане дуже актуальною, та перші проблеми можуть початися вже у 2020 році.

Як запобіжний захід може розглядатися зважене рішення власника системи щодо необхідності переходу на TLS 1.3 з врахуванням того, що TLS 1.2 не зламаний та поки не заборонений. Але рано чи пізно такий перехід відбудеться. Тому перед фахівцями по кібербезпеці постане питання: як здійснювати моніторинг трафіку, який неможливо моніторити? [4, 5]. Відповіддю на це питання може стати технологія, яка дозволяє без розшифровки зрозуміти, що знаходиться всередині зашифрованого трафіку, але без доступу до самого контенту (наприклад, технологія Cisco Encrypted Traffic Analytics).

Безфайлові атаки. Технології антивірусного захисту з'явилися наприкінці 80-х років і з тих пір глобально не змінювались. Існує шкідлива програма, її досліджують вірусні аналітики, розробляють сигнатуру та обладнують свої продукти. Якщо є сигнатура, то шкідлива програма нейтралізується, немає сигнатури, — не нейтралізується. Одною з задач зловмисників є залишатися якомога довше непоміченим. Для цього вони продовжують активно грати з системами безпеки. Дехто вдосконалює свою компетенцію щодо методів виявлення шкідливої та аномальної активності, інші нарощують потенціал якомога довше залишатися непоміченими. Однією з наростаючих тенденцій залишається застосування безфайлових атак, що активно експлуатують вбудовані в операційну систему (ОС) команди та PowerShell, видаючи себе за легітимних користувачів комп'ютера.

З огляду на те, що мова йде тільки про кінцеві пристрої, існують два типи рішення для нейтралізації названої загрози: системи захисту EDR та дозвіл збирати дані про активність на вузлі. Перший тип рішення (система EDR) дозволяє проводити інвентаризацію ПЗ, включаючи аналіз його вразливостей, блокувати експлойти, в тому числі і ті, що запускаються в пам'яті, аналізувати активність за рахунок індикторів компрометації, що постійно оновлюються, а також проводити розслідування та пошук загроз (threat hunting). Другий тип рішення дозволяє збирати дані про активність на вузлі в форматі адаптованого Netflow для її кореляції з даними, які отримуються на мережевому рівні.

Інтеграція, автоматизація та програмний інтерфейс API (Application Programming Interface). Інтеграція засобів безпеки не є забаганка виробників, а існуюча необхідність, продиктована зміною ландшафту загроз та виникненням багатовекторних атак, які проникають у корпоративні та відомчі мережі різними шляхами: через вразливості Web-порталів, підкинуті флешки, атаки Waterhole, через вразливий Wi-Fi, принесений заражений ноутбук керівника або підрядника тощо. Жодне рішення з інформаційної безпеки самотужки не здатне боротися із сучасними загрозами. Чекати, коли користувач самотійно почне інтегрувати придбані продукти в галузі інформаційної безпеки між собою — занадто довго та ненадійно. Сучасна тенденція інтеграції продуктів забезпечення безпеки інформації пояснюється бажанням виробників взяти цей процес у свої руки з метою належного контролю і уникнення конфліктних ситуацій та несумісності окремих продуктів.

За статистикою багато компаній використовують декілька десятків різних засобів захисту, які не в змозі взаємодіяти між собою, створюючи при цьому відчуття хибної захищеності. Час виявлення шкідливої активності всередині мережі сьогодні складає приблизно 200 діб. Це пов'язано з тим, що засоби захисту працюють незалежно один від одного (як держави на Балканах, звідки з'явився термін «балканізація Інтернет» як синонім створення національних сегментів Інтернет). Але ситуація буде змінюватися. І це вже можна спостерігати на прикладі компанії Cisco, яка поєднає дві сотні компаній-розробників, що об'єдналися з метою протистояти атакам, які постійно ускладнюються та прискорюються.

Адекватною відповіддю на зазначені загрози можуть стати автоматизація та API, які повинні бути реалізовані в усіх засобах захисту конкретної компанії-виробника з метою об'єднання їх у єдину систему захисту та отримання від цього синергетичного ефекту, що дозволить прискорити процес виявлення загроз від двох сотен діб до декількох годин. Це може бути досягнуто через обмін даними про загрози, за допомогою авто-

матизації створення сигнатур, отримання доступу з зовнішніх джерел індикаторів компрометації та передачі команд між засобами захисту тощо.

Використання штучного інтелекту. Автоматизація вирішення рутинних задач, прискорення повільних процесів, заміна кваліфікованих кадрів — ось декілька переваг застосування машинного навчання в інформаційній безпеці. З його допомогою можна виявляти шкідливий код і шкідливі домени та IP-адреси в Інтернет, фішингові атаки та вразливості, підвищувати обізнаність та ідентифікувати інсайдерів. Але штучний інтелект використовується не тільки на користь, але й на шкоду. Його освоїли зловмисники, які використовують машинне навчання для пошуку вразливостей та реалізації фішингових атак, обходу біометрії та створення фальшивих профілів в соціальних мережах, створення шкідливих програм, підбору паролів та обходу механізму CAPTCHA.

У 2018 році було представлено цікаві проекти зі створення фальшивих мастер-відбитків пальців, синтезу голосу, підміни обличчя на відео зображеннях, синхронізації руху губ з синтезованою мовою, накладання на чуже зображення у відеопотоці. Як показує практика нові технології швидко проникають у шахрайські та злочинні схеми, тому, поза сумнівом, це поставить перед фахівцями з інформаційної безпеки ряд нових питань з протистояння шкідливому використанню штучного інтелекту.

Засобом запобігання використанню штучного інтелекту у злочинних цілях є розробка нових та покращення існуючих механізмів машинного навчання у продуктах з кібербезпеки.

Багатофакторна автентифікація. Перелік факторів, що можуть ідентифікувати користувача:

- щось, про що ви знаєте (класичний пароль);
- щось, що ви маєте (біометрія); щось, що ви робите;
- щось, що ви загубили; щось, що ви забули; щось, що ви знайшли;
- щось, що ви бачили; щось, де вас бачили; щось, де ви були;
- щось, що ви створили; щось, що ви знищили; щось, що ви вкрали.

Насправді старі паролі, найпопулярнішим з яких протягом останніх п'яти років був «123456», відходять у минуле. Їм на заміну приходить дво- і багатофакторна автентифікація, яка дозволяє суттєво підвищити безпеку доступу користувачів до різноманітних сервісів та даних (корпоративним та приватним), які зберігаються всередині корпоративних центрів обробки даних (ЦОД) та за їх межами, у хмарах. Ми вже звикли використовувати вхід до зовнішніх сервісів через, наприклад, Facebook. Звикнемо і до використання двофакторної, а потім і багатофакторної автентифікації. На думку багатьох спеціалістів, це відбудеться у найближчому майбутньому. Проте біометрія навряд чи стане такою заміною, по-

заяк це не дуже дорого у порівнянні з іншими методами багатофакторної автентифікації та недоопрацьованості моделі загроз для неї.

На даний час існують компанії (наприклад Duo), які займаються активною розробкою та впровадженням засобів багатофакторної автентифікації.

Датацентричність. Багато компаній поступово відмовляються від периметру, відходячи у хмари та поступово запроваджуючи BYOD. Нікого не хвилює, зламують вашу мережу, чи ні. В разі зникнення даних на власника системи чекають негативні наслідки: регулятори, витік інформації до ЗМІ, звинувачення у некомпетентності. Надамо кількісний перелік витоків інформації (дані наведено у мільйонах записів):

Exactis — 340; Facebook — 50; Equifax — 145; Starwood — 500;
Yahoo — 3000; Under Armor — 150; Adult FriendFinder — 412;
MySpace — 164; Ebay — 145; Target — 110; Linkedin — 117;
Heartland Payment Systems — 130; Rambler — 98; TJX — 94;
AOL — 92; Quora — 100; VK — 100; Deep Root Analytics — 198;
JP Morgan Chase — 78; Mail.ru — 25; Anthem — 80;
Dailymotion — 85; Uber — 57; Tumblr — 65; Dropbox — 68;
Home Depot — 56; Adobe — 38; Sony PSN — 77; RSA Security — 40.

Зважаючи на цей перелік, можна припустити, що більша частина Інтернету втратила свої дані. Слід зазначити, що кількість інцидентів, у яких розмір витоку перевищує 10 млн записів, вимірюється вже не одиницями і навіть не десятками. Ситуація буде погіршуватися. ІТ спільнота приділяє занадто велику увагу захисту периметру, забуваючи про те, що безпека стала датацентричною, а не периметровою. І причиною цього є не тільки інциденти з даними, але й зростання регуляторного навантаження, пов'язаного із захистом персональних даних.

Адекватною відповіддю на зазначені виклики можуть стати засоби класифікації даних і боротьби з витоками та системи корпоративної кібербезпеки (наприклад, Cisco SAFE), які містять набір практичних рекомендацій щодо захисту різноманітних ділянок корпоративної мережі. Це стосується ЦОД, хмар, Wi-Fi, уніфікованих комунікацій тощо. Тільки захист всіх компонентів дозволить захистити дані від витоку, не виходячи за рамки законодавства.

Використання мереж 5G як плацдарму для атак. У США декілька міст заявили про те, що вони практично покрили свою територію мережами п'ятого покоління (5G), які дозволяють працювати в мережі Інтернет на швидкостях до 10 Гбіт/с. Це дозволить виключити «посередника»

у вигляді маршрутизатора, який зараз акумулює більшість з'єднань. В мережах 5G ситуація може змінитися, що значно збільшить площу нападу та зробить атаки на Інтернет речей більш масовими, як, власне, і використання Інтернету речей у якості плацдарму для атак, що дозволить значно збільшити потужність DDoS-атак.

Провідні компанії світу зараз працюють над розробкою рекомендацій та регламентів щодо протистояння загрозам у 5G-мережах та їх попередження.

Висновки

Враховуючи наведений аналітичний огляд найбільш актуальних кіберзагроз, можна зробити висновок, що у 2020 році особливу увагу слід приділити наступним кіберзагрозам:

- перехоплення трафіку через вразливості BGP;

- злами мережевих пристроїв;

- атаки на ланцюг поставок;

- вразливості протоколу TLS 1.3;

- безфайлові атаки;

- інтеграція, автоматизація та API;

- використання штучного інтелекту;

- датацентричність;

- використання мереж 5G як плацдарму для атак.

Рекомендації щодо захисту від кіберзагроз можуть бути наступні:

- коректне налаштування мережевого обладнання і моніторинг маршрутної інформації мережі;

- аналіз телеметрії, яка надходить від мережевого обладнання;

- моніторинг DNS;

- розробка нових та покращення існуючих механізмів машинного навчання у засобах кібербезпеки;

- багатофакторна автентифікація.

Лише комплексний підхід до захисту інформації, яка циркулює у мережах передачі даних підприємств енергетики, спроможний забезпечити необхідний рівень безпеки.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Thomas C. Reed *At the Abyss: An Insider's History of the Cold War*. Presidio Press, 2007, 386 p.
2. Регламент Європейського парламенту і Ради (ЄС) 2016/679 від 27.04.2016 «Про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних)». Брюссель, 2016, 98 с.
3. В.Л. Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Тольюпа Інформаційна та кібербезпека: соціотехнічний аспект: За заг. ред. д-ра техн. наук, проф. В.Б. Толубка. Київ: ДУТ, 2015, 288 с.
4. Виявлення зашифрованого трафіку шкідливих програм в контекстному потоці даних, Блейк Андерсон (Blake Anderson) та Девід Мак-Грю (David McGrew), конф. AISEC '16.
5. Аналітика зашифрованого трафіку. Офіційний документ. Загальнодоступна інформація Cisco, <https://www.cisco.com/> режимі доступу.

Отримано 17.10.19

REFERENCES

1. Thomas C. Reed (2007), "At the Abyss: An Insider's History of the Cold War", Presidio Press., 386 p.
2. (2016), "On the protection of individuals with regard to the processing of personal data and on the free movement of such data and on the repeal of Directive 95/46 / EC (General Data Protection Regulation)", *Regulation of the European Parliament and of the Council (EU)*, Brussels, Belgium.
3. Buryachok, V.L., Tolubko, V.B., Khoroshko, V.O. and Tolyupa, S.V. (2015), *Informatsiy-na ta kiberbezpeka: sotsiotekhnichnyy aspekt* [Information and cybersecurity: sociotechnical aspect], DUT, Kyiv, Ukraine, 288 p.
4. Anderson, B. and McGrew, D. "Detect encrypted malware traffic in the context data stream". *Proceeding of the AISEC '16 conferance*.
5. Analytics encrypted traffic. Official document. Cisco Public Information, available at: <https://www.cisco.com/> (June 16, 2019).

Received 17.10.19

М.Ю. Комаров

ОБЗОР КИБЕРАТАК НА ОБЪЕКТЫ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ

Дан аналитический обзор наиболее известных кибератак на объекты критической инфраструктуры. Представлен прогноз актуальных киберугроз на 2020 год.

К л ю ч е в ы е с л о в а: кибербезопасность, кибератака, уязвимость, компьютерный вирус, защита сети.

M.Y. Komarov

REVIEW OF CYBERATTACKS
ON OBJECTS OF CRITICAL INFRASTRUCTURE

An analytical review of the most famous cyber attacks on objects of critical infrastructure is given. A forecast of current cyber threats for 2020 is provided.

K e y w o r d s: cybersecurity, cyber attack, vulnerability, computer virus, network protection.

КОМАРОВ Максим Юрійович, аспірант, наук. співроб. Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України. У 2002 р. закінчив Національний технічний університет України «Київський політехнічний ін-т». Область наукових досліджень — кібербезпека об'єктів критичної інфраструктури, розробка методів та засобів забезпечення захисту інформації, що циркулює в інформаційно-телекомунікаційних системах підприємств енергетичної галузі.