Параметр	Опис
duration	тривалість з’єднання
protocol_type	тип протоколу (tcp, udp, та ін.)
service	мережева служба отримувача(http, telnet)
flag	стан з’єднання
src_bytes	число байтів переданих від джерела до отримувача
dst_bytes	число байтів переданих від отримувача до джерела
land	1 якщо з’єднання по ідентичним портам, 0 в інших випадках
wrong_fragment	кількість невірних пакетів
urgent	кількість пакетів з флагом urg

Завдання 8 полягає у виборі показників ефективності системи розпізнавання та алгоритмів оцінки їх значень. Для кожного класу кількість ознак варіюється від 3 до 9. Інформативність ознаки змінюється в діапазоні від -1 до +1. Для оцінки ефективності процедур розпізнавання можна використовувати метод ковзного контролю [3]. Під час тестування розробленого методу інтелектуального розпізнавання загроз, в якості вхідних даних для навчання та тестування використовувалася база даних KDD Cup Data.

Таким чином, ми проаналізували основні завдання, які необхідно вирішити в процесі проектування і побудови інтелектуальних систем розпізнавання кіберзагроз. Без їх вирішення не можлива побудова ефективно-функціонуючих систем інтелектуального розпізнавання образів в галузі кібербезпеки.

Список використаних джерел

1. Горелик А.Л., Современное состояние проблемы распознавания: Некоторые аспекты / А.Л. Горелик, И.Б. Гуревич, В.А. Скрипкин. – М.: Радио и связь, 1985. – 160с.

2. Петренко Т.А., Лахно В.А., Григорян Г.С. Розробка адаптивної системи розпізнавання кіберзагроз / Безпека українського суспільства в концепції вступу в постіндустріальне суспільство ЄС: Наукові доповіді та тези учасників науково-практичної конференції (м. Київ, 16 грудня 2015 р.), К., 2015. С. 66–76.

3. Мірошник, М. А. Розробка методів оцінки ефективності захисту інформації в розподілених комп'ютерних системах [Текст] / М. А. Мірошник // Інформаційно-керуючі системи на залізничному транспорті: науково-технічний журнал. – 2015. – № 4 (113). – С. 39–43.

УДК 004.8:004.056.54

ПРОТИДІЇ ШТУЧНОГО ІНТЕЛЕКТУ КІБЕРЗАГРОЗАМ

Плакса А.О., Соколовська А.А., студенти групи КБ-171
Усов Я.Ю., викладач кафедри кібербезпеки та математичного моделювання
Чернігівський національний технологічний університет

Вже давно стало зрозуміло, що компаніям потрібно в обов'язковому порядку реагувати на дедалі зростаючу кількість попереджень систем безпеки. А з урахуванням швидкості, з якою в 2018 році поширювалися по світу атаки вірусів-вимагачів, і все більш жорстких законодавчих вимог реакція повинна бути набагато швидшою. В умовах дефіциту відповідних фахівців компанії звертаються до засобів машинного навчання і штучного інтелекту для автоматизації процесів безпеки.

В контексті інформаційної безпеки **штучний інтелект** (artificial intelligence, AI) - це програмне забезпечення, здатне інтерпретувати стан середовища, розпізнавати в ній події і самостійно вживати необхідних заходів. AI особливо добре справляється з розпізнаванням закономірностей і аномалій, тому може бути прекрасним інструментом виявлення загроз.

Системи машинного навчання - це ПЗ, здатне самостійно навчатися на введених людиною даних і результатах виконаних дій. Засоби машинного навчання здатні будувати прогнози, спираючись на відомості про розвиток подій в минулому.

Застосування штучного інтелекту і машинного навчання для виявлення загроз.

У компаніях вже почали користуватися штучним інтелектом і машинним навчанням для розпізнавання загроз безпеки і реагування на них. З'явилися досить потужні інструменти, але потрібно визначитися, як включити їх в загальну стратегію кібербезпеки підприємства.

Наприклад, в банку Barclays Africa застосовують штучний інтелект для виявлення ознак компрометації систем в локальній корпоративній мережі і в хмарі. При цьому потрібна обробка гігантських обсягів даних, а в зв'язку з швидкою зміною світового ландшафту загроз і зростаючим взаємодією атакуючих, для протистояння їм необхідні найпередовіші технології та методи. Нарікаючи на гострий дефіцит фахівців, в банку зазначають, що вирішувати завдання безпеки вручну сьогодні вже просто неможливо.

За допомогою засобів штучного інтелекту від компанії Vectra Networks в Daqri ведуть моніторинг трафіку приблизно 1,2 тис. пристроїв, що працюють в корпоративному середовищі. Автоматизовані засоби здатні помітити, коли хтось виконує сканування портів, переходячи від хоста до хосту, або, припустимо, незвичайним способом пересилає великі обсяги даних. У компанії збирають всю відповідну інформацію, аналізують її і вводять в модель глибокого навчання. Завдяки цьому досягається можливість надійно прогнозувати ймовірність того, що той чи інший вид трафіку виявиться шкідливим.

Штучний інтелект і машинне навчання істотно прискорюють реагування на загрози, визнають аналітики Nemertes Research. За їх словами, сьогодні це вже серйозний ринок, сформований під впливом реальної потреби. У Nemertes провели глобальне дослідження, присвячене безпеці, і його результати свідчать: в середньому на виявлення атаки і реагування на неї в організаціях йде 39 днів, проте в деяких компаніях зуміли скоротити цей час до лічених годин. Швидкість реагування безпосередньо залежить від рівня автоматизації, яка забезпечується засобами AI і машинного навчання. Середній час виявлення атаки - годину. У найефективніших компаніях, які застосовують машинне навчання, на виявлення йде менше 10 хвилин, а в тих, що відстають - дні або тижні. Що стосується середнього часу аналізу загроз, воно становить три години. У кращих компаніях на такий аналіз йдуть хвилини, в гірших - дні або тижні. Поведінковий аналіз загроз вже застосовується в 21% компаній, які брали участь в опитуванні, і ще в 12% повідомляють, що впровадять відповідні кошти до кінця поточного року.

На передовій знаходяться компанії сфери фінансових послуг. Оскільки їх дані мають підвищену цінність, вони зазвичай з кібербезпеки йдуть на крок попереду всіх і вкладають значні кошти в нові далеко не дешеві технології.

Штучний інтелект дозволяє випередити зловмисників.

AI вдосконалюється в міру зростання обсягу отримуваних даних. При накопиченні досить великих зрізів даних системи здатні виявляти дуже ранні ознаки появи нових загроз. Приклад - SQL-ін'єкції. У компанії Alert Logic щоквартально збирають дані приблизно по 500 тис. Інцидентів, що відбуваються у 4 тис. її клієнтів. Близько половини таких інцидентів пов'язані з атаками на основі SQL-ін'єкцій. У жодній компанії світу немає можливості розглядати кожен такий інцидент окремо, щоб з'ясувати, чи вдалася спроба ін'єкції, впевнені в Alert Logic. Завдяки машинного навчання системи компанії не тільки швидше обробляють дані, але і корелюють події, що відбувалися в різні періоди часу в різних регіонах. Деякі атаки можуть повторюватися через кілька тижнів або місяців, при цьому виходити з інших сегментів Інтернету. Якби не машинне навчання, такі інциденти в Alert Logic упускали б, впевнені в компанії.

Великі обсяги інформації про загрози також збирають в GreatHorn, компанії, яка є оператором хмарного сервісу безпеки електронної пошти для Microsoft Office 365, Google G Suite і Slack.

Перспективи використання штучного інтелекту в світі безпеки.

Виявлення підозрілої активності користувачів і мережевого трафіку - найочевидніше застосування машинного навчання. Нинішні системи все успішніше справляються з виявленням незвичайних подій в великих потоках даних, рішенням стандартних завдань аналізу і розсилкою повідомлень. Наступний крок - використання AI для боротьби з більш складними проблемами. Наприклад, рівень кіберріска для компанії в кожен конкретний момент залежить від безлічі факторів, у тому числі від наявності систем без латок, незахищених портів, надходження повідомлень спрямованого фішингу, рівня надійності паролів, обсягу незашифрованих конфіденційних даних, а також від того, чи є організація об'єктом атаки з боку спецслужб іншої держави. Доступність точної картини ризиків дозволила б раціональніше використовувати ресурси і розробити більш детальний набір показників ефективності забезпечення безпеки. Сьогодні відповідні дані або не збираються, або не перетворюються на осмислені відомості, впевнені в компанії Balbix, що займається прогнозуванням ризику витоків даних з використанням штучного інтелекту. Фахівці компанії реалізували 24 види алгоритмів, які вибудовують «теплову карту» ризиків, що враховує всі особливості клієнтського середовища і дозволяє з'ясувати, чому та чи інша «гаряча» область позначена як така. При цьому сервіс видає поради щодо виправлення ситуації - якщо наслідувати їм, «гаряча» червона область стане спершу жовтої, потім зеленої. Системі також можна задавати питання на зразок «Що саме мені варто зробити в першу чергу?», «Який мій ризик фішингу?» Або «Який мій ризик виявитися жертвою WannaCry?». Надалі штучний інтелект буде допомагати компаніям визначатися, в які нові технології безпеки слід вкладатися. «У більшості компаній сьогодні не знають, скільки і як витрачати на кібербезпека, - впевнений Джеймс Стенгер, головний євангеліст технологій CompTIA. - Штучний інтелект потрібен, щоб виявити показники, на основі яких IT-директор зможе звернутися до керівника компанії або до ради директорів і пояснити, скільки і яких ресурсів потрібно для того чи іншого проекту, підкріпивши вимоги конкретними даними ».

Сьогодні AI використовується в безпеки дуже обмежено. Можна говорити про відставання від інших галузей, і навіть разюче, що самоврядні автомобілі з'являються раніше, ніж мережі, що захищають самі себе. Нинішні платформи AI ще по суті не "розуміють" навколишній світ. «Ці технології добре справляються з класифікацією даних, які схожі на зрізи і які використовувалися для навчання, - пояснює Стів Гробмен, директор за технологіями McAfee. - Але штучний інтелект не є по-справжньому розумним - він не може зрозуміти ідею, що лежить в основі тієї чи іншої атаки ». Тому людина як і раніше є ключовим елементом будь-якого рішення в області кіберзахисту.

І все ж прогрес в боротьбі з кіберзагрозами є. Існує такий напрямок досліджень, як генеративні змагальні мережі, - коли одночасно працюють дві моделі машинного навчання з протилежними цілями. Наприклад, одна намагається щось знайти, а інша - приховати те ж саме від виявлення. Цим принципом можна користуватися при створенні команд умовного противника, щоб з'ясовувати, якими можуть бути нові загрози.

Список використаних джерел

1. Ситуационные центры в решении проблем информационной безопасности [Електронний ресурс] – Режим доступу до ресурсу: http://www.itsec.ru/articles2/Inf_security/sit_cents [Назва з екрану].
2. Ротштейн А. П. Интеллектуальные технологии идентификации: нечеткие множества, генетические алгоритмы, нейронные сети / А. П. Ротштейн. – Винница : УНИВЕРСУМ – Винница, 1999. – 320 с.
3. Рябинин И. А. Надежность и безопасность структурно-сложных систем / И. А. Рябинин. – СПб.: Политехника, 2000. – 248 с. 9.
4. https://www.cio.ru/news/121117-Kak-iskusstvennyy-intellekt-mozhet-protivostoyat-kiberugrozam

---

УДК 004.056: 004.738.5

ВІДОМОСТІ ПРО ХАКЕРІВ ТА ХАКЕРСТВО

Реус О.А., студ. гр. АГ-181
Науковий керівник: **Гур'єв В.І.,** к.т.н., доцент
Чернігівський національний технологічний університет

Останніх 5-7 років в засобах масової інформації, а особливо в інтернет- виданнях ми чуємо інформацію про діяльність певної групи людей, які діяли разом або по одинці, яких називають "хакерами". На сьогоднішній день при дослідженні кримінального закону щодо злочинів у сфері використання ЕОМ, необхідно з'ясувати питання: хто ці люди? Чому вони вчиняють кримінально карані діяння? Повертаючись до історії, варто згадати про походження слова "хакер". В англійській мові дієслово "to hack" перекладається як "рубати, різати". Зародження хакерства знаменується не рядом зломів комп'ютерних систем чи баз даних, а дослідженням існуючої на початку 60-х років минулого століття при Масачусетському технологічному інституті комп'ютерної техніки та невтомних спроб молодих комп'ютерних геніїв створити машини на зразок тих, які знаходилися в стінах МТІ . Для того, щоб робота стала "хаком", вона повинна були мати технологічну новизну та новизну стилю. А якщо хтось говорив, що "хакерив" систему, то малося на увазі визнання майстерності в його діях. З часом найуспішніші члени клубу почали називати себе "хакерами". Що було особливою гордістю для них . Однак, програми, які писали хакери того часу не носили ознак правопорушень і застосовувались лише для вдосконалення своїх знань, вмінь та навичок. Досліджуючи можливості перших комп'ютерів, хакери дали поштовх для створення нової культури. Їхня етика говорила: "Доступ до комп'ютерів і до всього, що може дати нам знання про влаштування світу, повинен бути повним і необмеженим. Завжди дотримуйтесь Практичного Імперативу! ". В своїй діяльності хакери притримувалися думки, що необхідно розібрати досліджувану систему на частини, поспостерігати, як ці частини працюють, а потім використати ці знання, щоб створити нові, цікавіші речі. Хакери відкидали будь-які фізичні бар'єри, людей чи закони, які намагалися завадити у задоволенні жаги знань. Їхнім бажанням було покращити все те, що на їх думку працювало не досконало. Крім того, на переконання хакерів, для розвитку творчих здібностей повинен бути реалізований принцип вільного обміну інформацією, особливо комп'ютерними програмами.

Саме цей принцип став основою для вдосконалення програмного забезпечення та самовдосконалення самих хакерів і основою для створення хакерської етики. Для них було цінним мистецтво створення невеликих та функціональних програм. Проявом здібностей хакерів зламувати паролі стала система "Compatible Time-sharing System" (Сумісна система з розподілом часу), яка для роботи з собою вимагала авторизації – введення відповідного паролю. Оскільки хакери у своїй діяльності не визнавали, згідно з хакерською етикою, будь-яких обмежень, а інформація повинна бути доступною, ця система була об'єктом злому. Іншим таким же об'єктом діяльності хакерів стала система Miltics, система захисту якої була значно потужнішою. Виробники цієї системи вважали, що за користування останньою користувач повинен вносити плату, що суперечило етиці хакерів. Тому хакери "виснажували" цю систему різними хакерськими трюками.

В кінці 60-хроків хакерство почало поширюватися. Причиною цього було те, що ветерани МТІ залишали лабораторію і несли культуру в нові місця. Люди почали хотіти займатися хакерством, оскільки комп'ютери ставали доступнішими.

Крім МТІ осередком розвитку хакерства став Стенфордський університет, де молоді хакери творили історію розвитку хакерської етики. В цей час ARPA створила комунікаційну мережу комп'ютерів, на яку великий вплив мала хакерська етика. Вивчаючи розвиток хакерства та сучасний його стан, хакерство умовно можна поділити на "біле" хакерство та "чорне" хакерство. Такий умовний поділ не означає, що вони не вчиняють діянь, які становлять склад злочину, а визначається їх наслідками та такою складовою складу злочину як об'єкт. По своїй суті, "біле" хакерство передбачає дотримання хакерської етики, яка