УДК 004.56.5 + 004.89
В. І. Дорош, П. Ю. Якобчук, Едгарс Вейсс, А. В. Фаранович
Тернопільський національний економічний університет, Україна

ГЛИБОКІ НЕЙРОННІ МЕРЕЖІ ЯК ПЕРСПЕКТИВНИЙ НАПРЯМ ВИЯВЛЕННЯ АТАК В СУЧАСНИХ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ

V. Dorosh, P. Yakobchuk, E. Veiss, A. Faranovych
DEEP NEURAL NETWORKS AS A POWERFUL DIRECTION OF ATTACK DETECTION IN MODERN TELECOMMUNICATION NETWORKS

У зв'язку з постійно наростаючим використанням комп'ютерних систем у різних сферах науки, техніки, технологій, бізнесу, а також життя людей, інформаційні телекомунікаційні мережі піддаються різного роду загрозам, і користувач не може бути впевнений у захищеності важливої інформації, оскільки кіберзлочинці продовжують масово удосконалювати і розробляти методи і засоби організації кібератак (зловмисний код, мережеві вторгнення і т.д.).

У кіберпросторі 2016 рік видався напруженим і навіть бурхливим – від величезних ботнетів, що складаються з пристроїв інтернету речей, і шкідливих здирницьких програм до цільових кібершпіонських атак, крадіжок коштів у фінансових організацій, компаній і багато іншого. Звіт «Kaspersky Security Bulletin 2016. Статистика» містить детальну статистичну інформацію про актуальні загрози [0]:

– у 2016 році при роботі в інтернеті веб-атак шкідливих об'єктів класу «Malware» хоча б раз зазнали 31,9% комп'ютерів користувачів інтернету;

– рішення «Лабораторії Касперського» відбили 758044650 атак, які проводилися з інтернет-ресурсів, розміщених по всьому світу;

– зафіксовано 261774932 унікальних URL, на яких відбувалося спрацювання веб-антивірусу;

– веб-антивірусом було виявлено 69277289 унікальних шкідливих об'єктів (скрипти, експлойти, виконувані файли і т.д.);

– атаки шифрувальників відображені на комп'ютерах 1445434 унікальних користувачів;

– спроби запуску шкідливого ПЗ для крадіжки грошових коштів через онлайн-доступ до банківських рахунків відображені на комп'ютерах 2871965 користувачів;

– файловим антивірусом зафіксовано 116469744 унікальних шкідливих і потенційно небезпечних об'єктів.

Таким чином розробка ефективних методів захисту від комп'ютерних атак є надзвичайно актуальною, особливо в сучасних критичних телекомунікаційних мережах. Основною вимогою до виявлення атак в телекомунікаційних мережах критичного застосування є час виявлення атаки.

Сучасні комерційні системи виявлення комп'ютерних атак не забезпечують належний рівень захисту комп'ютерних систем, їх методи мають ряд недоліків. Так, найточніший на сьогодні метод, що ґрунтується на сигнатурному аналізі, добре функціонує при виявленні вже відомих комп'ютерних атак, але абсолютно не придатний для виявлення нових, раніше невідомих. А, як показує практика, саме нові, раніше невідомі, комп'ютерні атаки є причиною глобальних інформаційних катастроф і призводять до величезних фінансових і моральних збитків. Для захисту комп'ютерних систем від невідомих атак були розроблені різні евристичні методи. Але вони характеризуються високим рівнем помилок першого і другого роду (ймовірність пропуску атаки та ймовірність помилкових спрацювань), що ускладнює їх

застосування. Додатковим недоліком існуючих систем є їх висока обчислювальна складність.

Така ситуація стимулює розроблення нових підходів для виявлення комп'ютерних атак. Одним з перспективних напрямків є застосування методів штучного інтелекту. Проте, відомі підходи характеризуються наявністю ряду вузьких місць, таких як складність створення або вибору необхідних детекторів атак, громіздкість процедури адаптації до невідомих атак, здатність коректно працювати тільки на невеликих наборах даних, значна обчислювальна складність відомих методів, особливо в режимі реального часу, а також можливість відключення або спотворення функціонування під час атаки.

Перспективним є використання глибоких нейронних мереж, які мають велику ефективність нелінійного перетворення і представлення даних в порівнянні з традиційними нейронними мережами. Така мережа здійснює глибоке ієрархічне перетворення вхідного простору образів. Глибокі нейронні мережі, завдяки багатошаровій архітектурі дозволяють обробляти і аналізувати великий обсяг даних, а також моделювати когнітивні процеси в різних областях. В даний час більшість високотехнологічних компаній в США (Microsoft, Google, Facebook, Baidu і т.д.) використовують глибокі нейронні мережі для проектування різних інтелектуальних систем. За версією вчених Массачусетського технологічного інституту глибокі нейронні мережі входять в список 10 найбільш перспективних високих технологій, здатних в недалекому майбутньому в значній мірі перетворити повсякденне життя більшості людей на нашій планеті. Глибоке навчання стало однією з найбільш затребуваних областей інформаційних технологій. Перший шар мережі може отримати низькорівневі ознаки, другий шар − ознаки більш високого рівня і т.д. У загальному випадку глибока нейронна мережа є персептроном з великою кількістю прихованих шарів і дозволяє подолати обмеження класичного багатошарового персептрону завдяки глибокій архітектурі [0]. Глибоке навчання – це революційна техніка в області машинного навчання, яка успішно застосовується для вирішення багатьох проблем штучного інтелекту, наприклад, розпізнавання мови, комп'ютерний зір, обробка природної мови, візуалізація даних і т.д. Глибока нейронна мережа (deep neural networks) складається з безлічі прихованих шарів і дозволяє виконувати глибоке ієрархічне перетворення вхідних даних [3–5]. Такі переваги глибоких нейронних мереж дозволяють використовувати їх і для побудови систем виявлення атак в сучасних телекомунікаційних мережах [6].

Література

1. Kaspersky Security Bulletin 2016. Статистика [Електронний ресурс] – Режим доступу : https://go.kaspersky.com/RU_Security_Bulletin_2016_Stats_ SOC_2016.html.

2. Головко В.А. Метод обучения нейронной сети глубокого доверия и применение для визуализации данных / В.А. Головко, А.А. Крощенко // Комп'ютерно-інтегровані технології: освіта, наука, виробництво. – 2015. – № 19. – С. 6–12.

3. Hinton G. E. A fast learning algorithm for deep belief nets / G. E. Hinton, S. Osindero, Y. Teh // Neural Computation. – 2006. – Vo1. 18. – P. 1527-1554.

4. Hinton G. Reducing the dimensionality of data with neural networks / G. Hinton, R. Salakhutdinov // Science. – 2006. – Vo1. 313 (5786). – P. 504-507.

5. LeCun, Y., Bengio, Y., Hinton, G. Deep learning / Y. LeCun, Y. Bengio, G. Hinton // Nature. – 2015. − 521 (7553). – P. 436–444.

6. Скумін Т. Застосування нейронних мереж глибокої довіри для виявлення комп'ютерних атак / Т. Скумін, В. Головко, А. Саченко, М. Комар // Збірник тез V Міжнародної науково-технічної конференції «Захист інформації і безпека інформаційних систем». – Львів, Україна, 2-3 червня, 2016. – С. 162-164.