ӘОЖ 004.032.26

НЕЙРОНДЫҚ ЖЕЛІЛЕР АРҚЫЛЫ CHROME БРАУЗЕРІНДЕГІ ВИРУСТАРДЫ АНЫҚТАУ

Нұрмұханбетова Альбина Ерланқызы
nuralbina9898@gmail.com
Л.Н.Гумилев атындағы ЕҰУ, «Радиотехника, электроника және телекоммуникация» кафедрасының магистранты, Нұр-Сұлтан, Қазақстан
Ғылыми жетекшісі – А.Е. Наурызбаев

Көптеген зерттеулерге сәйкес, зиянды бағдарламалар қазіргі таңдағы жалпы және арнайы мақсаттар үшін қолданылатын компьютерелер жүйесіндегі ұзақ уақыт бойы қауіптердің бірі болып табылынады [1,2,3,4]. Бұл туралы әртүрлі зиянды бағдарламалардың көмегімен жасалынған сәтті кибершабуылдар дәлел бола алады [5]. Бірқатар эксперттер тиісті қауіпсіздік құралдарын жасаумен айналысуда, алайда мәселе әлі шешімін таппады. Зиянды бағдарламалар компьютерлің жүйеге енген уақытта ғана негізгі мәселелер басталады.

Бұл мақсат үшін заманауи қорғаныс жүйелері нейрондық желілермен қатысты теорияны үлкен масштабта қолдануда. Осы бағыттың болашақтағы перспективалары нейрондық желілерді қолдану арқылы компьютерлік вирустарды анықтау (ашық кодқа ие антивирустық бағдаралама ClamAV, Deep Instinct іске қосу) және үлкен көлемдегі теориялық және практикалық жұмыстардың көптігімен жалпыланады [6].

Сонымен қоса, анықтау дәлдігінің жеткіліксіздігі және пайдалану жағдайларына бейімделудің нашарлығы, сондай-ақ қолданылатын шешімдердің жабық сипаты олардың қолданылу аясын едәуір шектейді, ал нейрондық желілер теориясының үнемі ілгерілеуі зиянды бағдарламаларды анықтау үшін дәлелденген нейрондық желі құралдарының (NNT) айтарлықтай жақсаруы мүмкін екендігін көрсетеді. Бұл қазіргі нейрондық желілердің құралдар жиынтығын жақсарту үшін зерттеулердің өзектілігін түсіндіреді, бұл заманауи теориялық шешімдерді қолдану арқылы зиянды бағдарламаларды тиімді анықтауға мүмкіндік береді.

Зиянды бағдарламаларға қарсы шаралар екі түрге бөлінеді. Біреуі – терминалдардың жұқтырылуын болдырмау үшін зиянды файлдарды орындалмас бұрын анықтау, екіншісі – инфекцияның таралуын азайту үшін зарарланған терминалдарды анықтау.

Инфекцияны болдырмауға қарсы шара ретінде зиянды файлдарды немесе бағдарламаларды табу олардың қолтаңбасы немесе әрекеті арқылы анықталады. Қолтаңбаға негізделген анықтау қатесінің жиілігі өте төмен болғанымен, ол алдын ала қол қою талабына байланысты белгісіз зиянды бағдарламаға бейімделе алмайды. Бұл мәселені шешу үшін мінез-құлыққа негізделген анықтау әдісі ұсынылды. Бұл әдіс зиянды бағдарламалар файлдарын мінез-құлық немесе құрылымдық мүмкіндіктері негізінде табады.

Ахмед және тағы да басқа зерттеушілер API қоңырауларының кеңістіктік немесе уақыттық мүмкіндіктеріне негізделген зиянды файлдарды анықтау әдісін ұсынды [7]. Олар API шақыруларының кеңістіктік ақпаратынан алынған аргументтер мен қайтаратын мәндер сияқты функцияларды және API қоңырауларының реттілігі сияқты уақытша ақпаратты пайдаланады. Кеңістіктік ақпараты статистикалық талдау немесе ақпараттық-теориялық әдіс арқылы шығарылады. Уақытша ақпарат Марков тізбегін пайдаланып, API шақыру ретін модельдейтін өтпелі матрица арқылы есептелінеді.

Казіргі кезде инфекцияға қарсы шаралардың бөлігі ретінде трафик деректері бойынша көптеген зерттеулер бар. Бірнеше ғалымдардың тұжырымдамасы бойынша трафиктің пайдалы жүктемесінде ASCII кодының пайда болу жиілігін және HTTP сұрауының ұзақтығын пайдаланып, зиянды бағдарламаның инфекциясын анықтауға болады [8]. Олар, сондай-ақ, сериялық функцияны зиянды және қалыпты трафик арасында ерекшеленетінін айтады. Дегенмен, мінез-құлыққа негізделген анықтау әдісінің анықтау қателігі жоғарырақ болады. Оның үстіне, тек трафик деректеріне негізделген әдісті пайдалану жеткіліксіз, өйткені соңғы зиянды трафик әртараптандырылған және зиянды трафик азырақ анықталатын көрсетті.

Нейрондық желі (Neural Network) – бұл мидың желілік құрылымын модельдейтін математикалық модель. Нейрондық желілер нейрондардың көптеген қабаттарынан тұрады. Конволюцилық нейрондық желі (Convolutional Neural Network) – бұл нейрондық желінің көптеген жасырын қабаттарынан тұрады. Ол кескіндерді тану және тілді өңдеу сияқты әртүрлі салаларды өзіне қаратады, яғни бұл нейрондық желі функциялар мен дерексіз функцияларды автоматты түрде біле алады.

Хинтон және тағы да басқа зерттеушілер конволюциялық нейрондық желінің өнімділігін жақсартатын скринингті ұсынды [9]. Бұл әдіс нейрондар арасындағы тәуелділікті азайтады, шамадан тыс сәйкес келмеу үшін нейрондардың кейбір нәтижелерін алып тастайды.

Шығарылған нейрондар әр кіріс сигналы үшін кездейсоқ таңдалады. Осылайша, әр жаттығу әр түрлі құрылымдық желіні қолдана отырып жасалады және бұл нейрондар арасындағы тәуелділікті азайтады.

Конволюциялық нейрондық желінің негізгі екі арнайы қабаты бар, мысалы, жинақтау қабаты және біріктіру қабаты. Жинақтау қабатында нысандар кіріс сүзгісінің көмегімен алынады. Біріктіруші қабатта позицияның аздап ығысуының әсерін азайту үшін кірістер іріктеумен таңдалады.

Конволюциялық нейрондық желілер екі түрлі арнайы қабаттардың бірнеше жиынтығынан және қарапайым нейрондық желілердің жиынтығынан тұрады. Бұл нейрондық көп аса кескіндерді тануда қолданылады, себебі бұл желі нысандарды олардың орналасуына қарамастан тани алады. Крижевский және тағы да басқаларды бір таңқалдырғаны, конволюциялық желілердің [10] көмегімен объектілерді тану туралы мәліметтер жиынтығындағы қателіктер азайды.

Қайталанатын нейрондық желілерде алдыңғы кірістерді немесе жасырын қабаттардың күйі туралы ақпаратты сақтайтын арнайы цикл құрылымы немесе жад блоктары бар. Қайталанатын нейрондық желілер деректердің тізбегін үйрете алады, себебі олардың шығыстары алдыңғы кірістерге тәуелді. Бұл нейрондық желіде жаттығу кезеңінде кіріс тізбегінің ұзақ уақыт кері таралуымен қате жиі жоғалады деген мәселе бар. Бұл мәселені болдырмау үшін Герс және басқа зерттеушілер LSTM (long short term memory – ұзақ қысқа мерзімді жад) ұсынды [10].

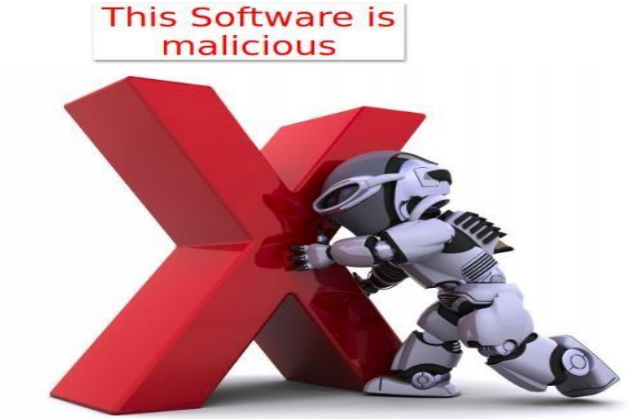
Бұл қателіктердің жойылып кету мәселесінен аулақ болу үшін жасырын қабаттардың салмағын бекіту арқылы қателердің жойылып кетуінің алдын алады және болашақ деректер үшін кіріс мәліметтердің барлығын қарастырмай, тек қана таңдалған мәліметтерді сақтайды. Қайталанатын нейрондық желі тілді өңдеу немесе сөйлеуді тану сияқты деректердің тізбегін қолданатын әртүрлі салаларда жақсы нәтижелер көрсетуде.

Миколов және тағы да басқа зерттеушілер қарапайым қайталанатын нейрондық желіні қолданатын қайталанатын нейрондық желінің тілдік моделін қарастырды [6]. Тілдік модельдеудің мақсаты алдыңғы кірістерге негізделген келесі сөзді болжау болып табылады. RNNLM (Recurrent Neural Network Language Model – қайталанатын нейрондық желі тілі моделі)-де сөздер потенциалды векторларға айналады, ал келесі сөзді ағымдағы енгізу сөзінің ықтимал векторы және алдыңғы енгізу тарихы болжайды. С өздің семантикалық ақпараты потенциалды векторда сақталады және сөздер арасындағы байланысты осы потенциалды векторды қолдана отырып есептеуге болады. Паскан және тағы да басқа зерттеушілер қайталанатын нейрондық желінің [7] көмегімен зиянды бағдарламаларды анықтау әдісін ұсынды.

Олар алдымен қайталанатын нейрондық желіні API (Application Programming Interface – қосымшаның программалау интерфесі) қоңырауларының тілдік моделін құруға үйретеді, одан соң әр уақыт сайын алынған жасырын векторды түрлендіру арқылы бекітілген ұзындықтағы объект векторларын жасайды.

Содан кейін сипаттама векторлары логистикалық регрессия немесе көп қабатты перцептрон арқылы жіктеледі.

Сурет 1 – Жүйеде вирус анықталмады



Сурет 2 – Жүйеде вирус анықталды

Вирустарды анықтауда нейрондық желілерді қолданудың маңыздылығы өте зор. Нейрондық желілердің көмегімен зиянды бағдарламаларды немесе вирустарды оңай анықтауға болады. Бұл мақсат үшін Python бағдарламалау тілі пайдаланылады. Python-дағы кодты жетілдіру және жасау арқылы вирустардың бар-жоғын көрсететін нәтижелер болады.

Қолданылған әдебиеттер тізімі:

1. Ahmadi, M., Ulyanov, D., Semenov, S., Trofimov, M., Giacinto, G.: Novel feature extraction, selection and fusion for effective malware family classification. In: Proceedings of the Sixth ACM Conference on Data and Application Security and Privacy (CODASPY 2016) // New York, NY, USA .2016. P. 183–194.

2. Bapiyev, I.M., Aitchanov, B.H., Tereikovskyi, I.A., Tereikovska, L.A., Korchenko, A.A.: Deep neural networks in cyber attack detection systems.// Int. J. Civil Eng. Technol. (IJCIET). 2017 №8. P.1086–1092.

3. Lakhno, V., Malyukov, V., Parkhuts, L., Buriachok, V., Satzhanov, B., Tabylov,

A.: Funding model for port information system cyber security facilities with incomplete Hacker // J. Theor. Appl. Inf. Technol. 2018 №13. P. 4215–4225.

4. Rudenko, O.H., Bodianskyi, Ye.: Artificial neural networks. // Kompaniia SMIT. 2016. P. 404.

5. Shah, S., Jani, H., Shetty, S., Bhowmick, K.: Virus detection using artificial neural networks // Int. J. Comput. 2013 №5. P 17–23.

6. Falaye, A.A., Oluyemi, E.S., Victor, A.N., Uchenna, U.C., Ogedengbe, O., Ale, S. Parametric equation for capturing dynamics of cyber attack malware transmission with mitigation on computer network //Int. J. Math. Sci. Comput. (IJMSC).2014. №4. P37–51.