APJ. 5(2):1-15, Summer 2024

Arman Process Journal (APJ)

Arman Process Journal (APJ)

Homepage: https://www.armanprocessjournal.ir

Analysis of Failed DNS Responses Using Neural Network in Botnet Detection

V. Mohammadi[*,1], M. Shirmohammadi[2]

[1] Department of Information Technology Management, Hamedan Branch, Islamic Azad University, Hamedan, Iran
[2] Department of Computer Engineering, Hamedan Branch, Islamic Azad University, Hamedan, Iran

RESEARCH PAPER

Received: 2 April 2024
Accepted: 24 June 2024

KEYWORDS:
Botnet,
Command and Control Server,
DNS Traffic,
Nxdomain,
Neural Network

[1] **Corresponding author:**
Vahid.mohammadi1364@gmail.com

ABSTRACT

With the increasing development of technology and the expansion of the use of the Internet, botnets are considered as one of the most important security threats in the digital space. Botnets are networks of infected devices controlled by attackers and used for various purposes such as sending spam, DDoS attacks, and stealing sensitive information. Considering the increasing trend of using botnets, it is very important to detect and prevent their activity. The spread of communication, resource sharing, curiosity, earning money, gathering information and gaining resource capacity are motivations for creating botnets. In addition to these, political, economic and military motives should also be added. Our method has the ability to detect known and unknown botnets that use this method. Our goal in this paper is to present an innovative method to detect botnets using failed response analysis and neural network. In this method, botnets are detected based on failed responses or NXDomain in each host. This feature increases the accuracy of detection in small and medium networks. This method has been tested in networks infected with Konfiker and Kraken botnets and the information obtained from it has been analyzed using neural networks. The evaluation results show the good performance of this method in botnet detection.

نشریه تخصصی آرمان پردازش، دوره ۵، شماره ۲، تابستان ۱۴۰۳

فصلنامه تخصصی آرمان پردازش
(APJ)
Homepage: www.armanprocessjournal.ir

فصلنامه تخصصی فناوری اطلاعات و ارتباطات
شماره مجوز: ۸۷۰۹۰

آنالیز پاسخهای ناموفق DNS با استفاده از شبکه عصبی در تشخیص بات نت

وحید محمدی*[۱]، محمد مهدی شیرمحمدی[۲]

[۱] گروه مدیریت فناوری اطلاعات ،واحد همدان ، دانشگاه آزاد اسلامی، همدان، ایران

[۲] گروه مهندسی کامپیوتر ،واحد همدان ، دانشگاه آزاد اسلامی، همدان، ایران

چکیده

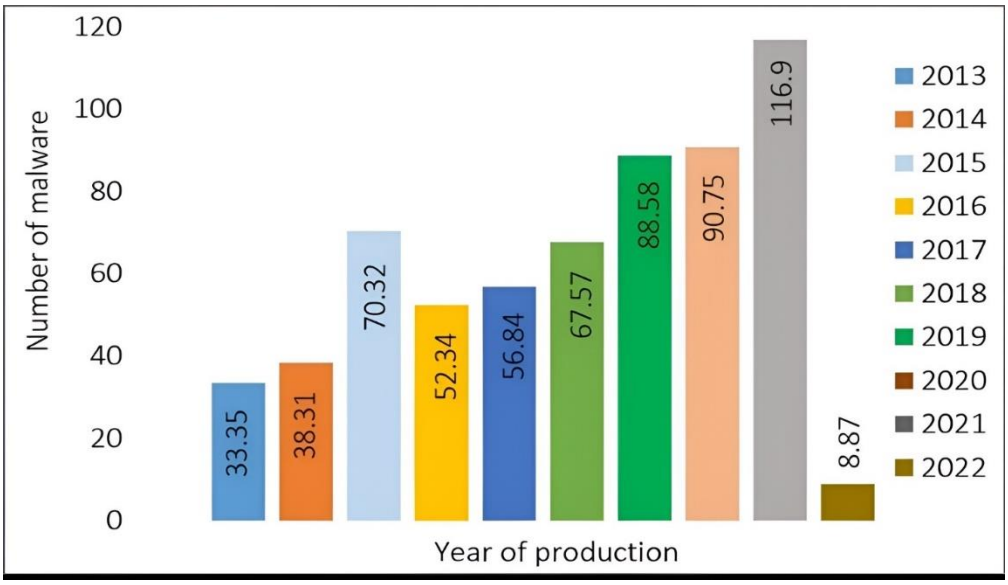
مقاله پژوهشی

واژگان کلیدی:
بات نت،
سرور فرماندهی و کنترل،
ترافیک سرویس نام دامنه،
پاسخ‌های ناموفق،
شبکه عصبی،

با پیشرفت روزافزون فناوری و گسترش استفاده از اینترنت، بات نت ها به عنوان یکی از تهدیدات امنیتی مهم در فضای دیجیتال به شمار می‌روند. بات نت ها، شبکه‌هایی از د ستگاه‌های آلوده‌اند که تو سط مهاجمان کنترل می شوند و برای اهداف مختلفی مانند ارسال اسپم، حملات DDoS و سرقت اطلاعات حساس استفاده می‌شوند. با توجه به روند رو به افزایش اســتفاده از بات نت ها، تشــخیص و جلوگیری از فعالیت آن‌ها از اهمیت بســیاری برخوردار اســت. گســتردگی ارتباطات، به اشتراک گذاری منابع، حس کنجکاوی، کسب پول، جمع آوری اطلاعات و به دست آوردن ظرفیت منابع، انگیزه هایی برای ایجاد بات نت است .علاوه بر اینها باید انگیزه های سیاسی، اقتصادی و نظامی را نیز اضافه نمود.روش ما قابلیت ت شخیص بات نت ها ی شناخته شده و همچنین نا شناخته ای که از این روش ا ستفاد می کنند را دارا هست.هدف ما در این مقاله، ارائه روشی نوآورانه برای تشخیص بات نت ها با استفاده از تحلیل پاسخ‌های ناموفق و شبکه عصــبی اســت. در این روش تشــخیص باتنت‌ها براســاس پاســخ‌های ناموفق یا NXDomain در هر میزبان صــورت می‌گیرد. این ویژگی باعث می‌شــود که دقت تشــخیص در شــبکه‌های کوچک و متوســط افزایش یابد. این روش در شبکه‌های آلوده به باتنت‌های کانفیکر و کراکن آزمایش و اطلاعات به‌د ست‌آمده از آن با ا ستفاده از شبکه‌های ع صبی مورد تجزیه‌وتحلیل قرارگرفته است. نتایج ارزیابی نشان‌دهنده کارایی خوب این روش در تشخیص باتنت است.

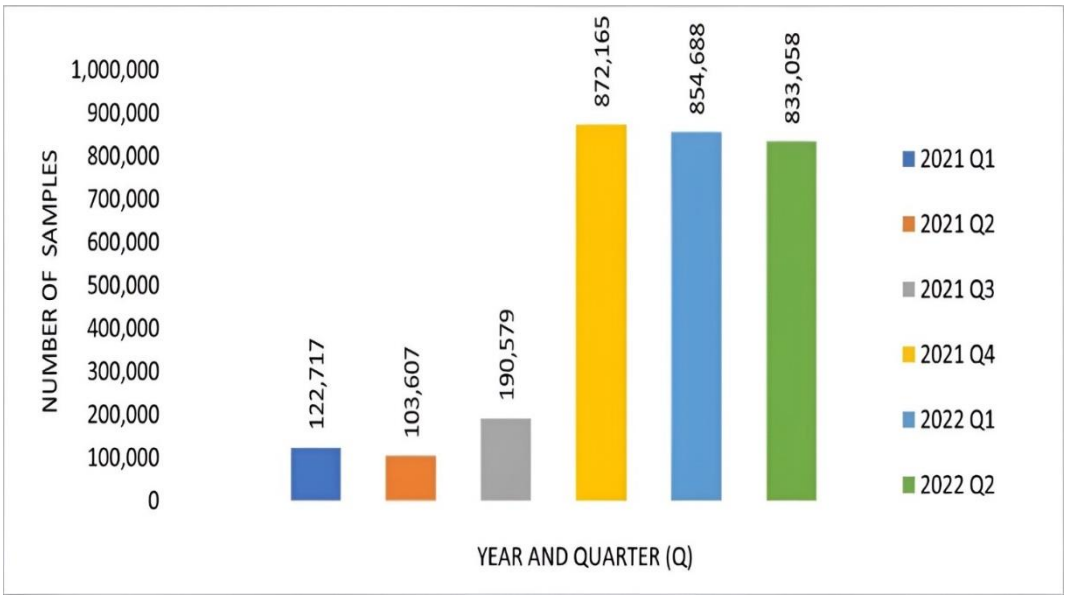
مقدمه

بدافزارها یکی از رایج ترین و شدیدترین حملات سایبری امروزی هستند .بدافزار میلیون‌ها دستگاه را آلوده می‌کند و می‌تواند چندین فعالیت مخرب از جمله استخراج داده‌های حساس، رمزگذاری داده‌ها، فلج کردن عملکرد سیستم و بسیاری موارد دیگر را انجام دهد .از این رو، تشخیص بدافزار برای محافظت از رایانه ها و دستگاه های تلفن همراه ما در برابر حملات بدافزار بسیار مهم است. ترافیک بدافزار همیشه نامتقارن است در مقایسه با ترافیک خوش خیم که همیشه متقارن است .خوشبختانه تکنیک‌های هوش مصنوعی زیادی وجود دارد که می‌توان برای شناسایی بدافزارها و تمایز آن‌ها از فعالیت‌های عادی استفاده کرد .با این حال، مشکل برخورد با داده های بزرگ و با ابعاد بالا به اندازه کافی مورد توجه قرار نگرفته است.بدافزارها بر بسیاری از ابزارهای محاسباتی در عصر دیجیتال تأثیر گذاشته اند .نرم افزارهای بدخواه یا بدافزار با هدف دستیابی به اهداف منفی یک مهاجم مخرب ایجاد می شود .بدافزارها می‌توانند به شبکه‌ها حمله کنند، به زیرساخت‌های حیاتی آسیب بزنند، رایانه‌ها و دستگاه‌های هوشمند را در معرض خطر قرار دهند و داده‌های حساس را به سرقت ببرند. آمار توسعه بدافزار درسیستم عامل ویندوز و لینوکس که توسط بخش تحقیقاتی موسسه ای-وی تست (AV-Test) انجام شده و در شکل۲و۳ قابل مشاهده است مهر تاییدی بر این موضوع را دارد [۱] .



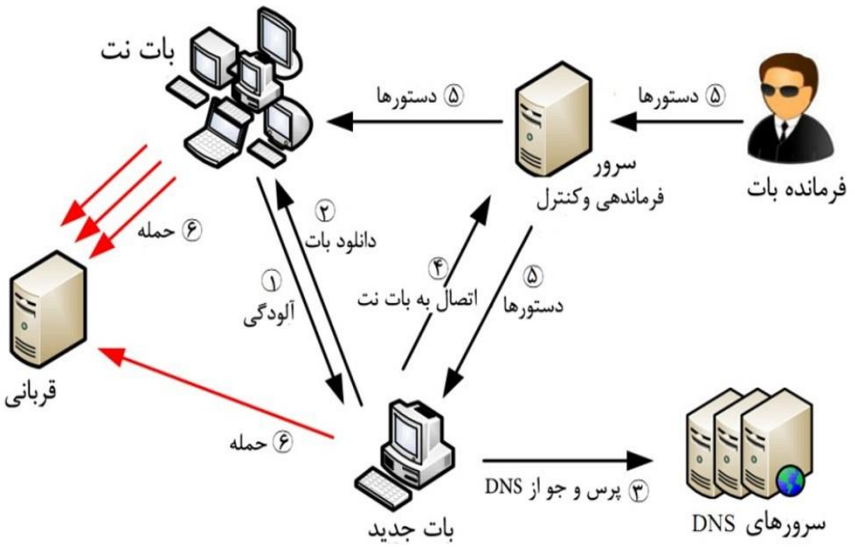
شکل ۱: توسعه بدافزار در (الف) ویندوز از 2013-Feb 2022 AV-TEST (2022)

با افزایش حملات اینترنتی، به دلایلی همچون مسائل سیاسی، اقتصادی، اجتماعی، نظامی و غیره و همچنین شیوع استفاده از بات نت ها، آن‌ها ابزاری خطرناک که دارای قدرت تخریبی بسیار بالایی هستند تبدیل‌شده‌اند. همچنین پیشرفت بات نت‌ها و انتقال آن‌ها از معماری قدیم (HTTP,IRC) به معماری جدید (P2P) تشخیص آن‌ها را سخت نموده است [۲۰] . در چند ده اخیر شاهد افزایش استفاده از اینترنت و برنامه‌های کاربردی آن هستیم، به صورتی که استفاده از اینترنت به بخش مهمی در زندگی روزمره ما تبدیل‌شده است. اگرچه اینترنت تسهیلات زیادی را به ما ارائه می‌دهد، اما با افزایش استفاده از اینترنت چالش‌های امنیتی بزرگی ظاهرشده است و این امر به مسئله‌ی مهم و حساسی برای بسیاری از اشخاص و شرکت‌ها تبدیل‌شده است. بسیاری از حملات و فعالیت‌های جعلی در اینترنت از طریق نرم‌افزارهای مخرب انجام می‌شود، این نرم‌افزارها شامل ویروس‌ها، اسب‌های تروجان و کرم‌ها است که در چند سال اخیر بات نت ها نیز به این مجموعه اضافه شده است. بات نت‌ها به یک منبع اساسی برای بسیاری از حملات خطرناک از قبیل پویش، جلوگیری از سرویس توزیع‌شده، هرزنامه، فعالیت‌های جعلی و غیره تبدیل‌شده‌اند[۲۲-۲۱] .



شکل ۲: رشد خانواده بدافزار لینوکس از 2021 Q1-2022 Q2, data from C. (2022)

دو عامل مهم در افزایش سوءاستفاده حمله‌کنندگان مؤثر است ۱) کاربران ناآگاه و ۲) وجود آسیب‌پذیری‌های متعدد در نرم‌افزارها. باوجوداین دو عامل، نفوذ گران کامپیوتری صرف‌نظر از محل جغرافیایی خود و یا کاربر می‌توانند به دستگاه‌های مختلف حمله کنند و از آن‌ها سوءاستفاده نمایند. در چنین شرایطی امنیت به‌عنوان مسئله‌ای مهم پدیدار می‌شود.واژه امنیت عبارت است از به حداقل رساندن آسیب‌پذیری منابع و سرمایه‌ها. اگر بخواهیم تعریف دقیق‌تر و رسمی‌تری از امنیت بیان نماییم باید بگوییم که امنیت مبتنی بر تحقق سه ویژگی محرمانگی، جامعیت و دسترس‌پذیری در یک سیستم است. محرمانگی این اطمینان را به فرستنده می‌دهد؛ که تنها گیرنده‌ی موردنظر وی توانایی درک داده‌ها را داشته باشد و سایر عوامل موجود در سیستم که مجاز به دسترسی به آن اطلاعات نیستند، نتوانند محتویات فرستاده‌شده را تشخیص دهند. جامعیت تضمین می‌کند که اطلاعات سیستم با تلاش‌های غیرمادی و یا عمدی و بدخواهانه بدون تغییر باقی بماند و دسترس‌پذیری نیز بدان معناست که اطلاعات و منابع سیستم در هر زمان، در هر جا و به هر شکل که کاربران نیاز دارند، در دسترس آن‌ها قرار گیرد. به‌عبارت‌دیگر سیستم باید عملیاتی باشد و سرویس‌ها را به‌درستی ارائه دهد و ارائه هیچ‌یک از سرویس‌ها را انکار ننماید. یکی از تهدیدات روزافزون در اینترنت و شبکه‌های کامپیوتری که اصل دسترس‌پذیری را نقض می‌کند Botnet است که به‌عنوان مهم‌ترین تهدیدکننده امنیتی در چند سال اخیر شناخته‌شده است.



شکل۳:چرخه زندگی و ساختار یک بات نت بر پایه IRC برگرفته از [۲۳]

شکل۳ چرخه زندگی و ساختار یک بات نت را نشان می دهد: در دنیای امروز، با توجه به پیشرفت روزافزون فناوری و افزایش وابستگی به اینترنت، امنیت شبکه به یکی از مهم‌ترین چالش‌های حوزه فناوری اطلاعات تبدیل شده است. یکی از بزرگترین تهدیدات امنیتی در این زمینه، باتنت‌ها هستند. یکی از روش‌های موثر برای تشخیص باتنت‌ها، تحلیل پاسخ‌های ناموفق یا NXDomain در شبکه است. باتنت‌ها غالباً با ارسال حجم زیادی از درخواست‌های شبکه که منجر به پاسخ‌های ناموفق می‌شود، قابل شناسایی هستند. این رفتارهای غیرعادی می‌تواند به عنوان نشانه‌ای از وجود باتنت‌ها در شبکه مورد استفاده قرار گیرد. با پیشرفت در حوزه تکنولوژی های هوش مصنوعی و یادگیری ماشین، استفاده از شبکه‌های عصبی برای تحلیل و تشخیص الگوهای پیچیده در داده‌های شبکه به یک رویکرد موثر تبدیل شده است. شبکه‌های عصبی با توانایی بالای خود در یادگیری و تشخیص الگوهای غیرخطی، می‌توانند برای شناسایی رفتارهای غیرعادی ناشی از باتنت‌ها بسیار کارآمد باشند [۱۸].

تجزیه و تحلیل کارهای مرتبط:

برای تشخیص بات نت‌ها روش‌های مختلفی پیشنهادشده است که در ادامه به برخی از آن‌ها اشاره می‌شود. YU و همکاران [۳۰] یک روش مبتنی بر استفاده از شبکه‌های عصبی عمیق (DNN) برای تحلیل ترافیک DNS و تشخیص باتنت‌ها ارائه کرده‌اند. دقت بالا در تشخیص باتنت‌ها به دلیل توانایی شبکه‌های عصبی در شناسایی الگوهای پیچیده و نامنظم ترافیک شبکه وهمچنین قابلیت یادگیری خودکار ویژگی‌ها بدون نیاز به استخراج دستی از نقاط قوت این روش می باشد. نیاز به حجم بالایی از داده‌های آموزشی برای آموزش شبکه‌های عصبی و همچنین زمان و منابع محاسباتی زیاد برای آموزش و اجرای مدل‌ها از نقاط ضعف این روش می باشد.

Bilge و همکاران [۳۱] یک روش مبتنی بر استفاده از از الگوریتم‌های ماشین یادگیری سنتی مانند جنگل تصادفی (Random Forest)و ماشین بردار پشتیبانی (SVM) برای تحلیل ترافیک DNS و تشخیص باتنت‌ها ارائه کرده‌اند. پیاده‌سازی و آموزش ساده‌تر الگوریتم‌های ماشین یادگیری سنتی وهمچنین نیاز به داده‌های کمتر نسبت به شبکه‌های عصبی از نقاط قوت این روش می باشد. دقت پایین‌تر نسبت به شبکه‌های عصبی در تشخیص باتنت‌هاو همچنین قابلیت یادگیری محدودتر و نیاز به استخراج دستی ویژگی‌ها از نقاط ضعف این روش می باشد.

Antonkakis و همکاران [۲۹] یک روش مبتنی بر استفاده از شبکه‌های عصبی بازگشتی (RNN) برای تحلیل توالی‌های زمانی درخواست‌های DNS و شناسایی الگوهای غیرمعمول برای تشخیص باتنت‌ها ارائه کرده‌اند. دقت بالا در شناسایی الگوهای زمانی پیچیده وهمچنین قابلیت مدل‌سازی توالی‌های زمانی و شناسایی رفتارهای غیرمعمول از نقاط قوت این روش می باشد. پیچیدگی در پیاده‌سازی و آموزشRNN هاو همچنین نیاز به داده‌های برچسب‌گذاری شده برای آموزش مدل‌ها از نقاط ضعف این روش می باشد.

Wang و همکاران [۲۸] از چندین تکنیک ماشین لرنینگ شامل شبکه‌های عصبی استفاده کرده و نشان می‌دهد که این تکنیک‌ها در تشخیص باتنت‌ها دقت بالایی دارند. استفاده از چندین تکنیک، استفاده از داده‌های واقعی، دقت بالااز نقاط قوت این روش می باشد. عدم تمرکز بر پاسخ‌های ناموفقDNS ، پیچیدگی بیشتراز نقاط ضعف این روش می باشد. Lu و همکاران [۲۷] از شبکه‌های عصبی LSTM برای تحلیل ترافیک DNS استفاده کرده و نشان می‌دهد که LSTM می‌تواند الگوهای پیچیده را شناسایی کند. استفاده از LSTM برای شناسایی الگوهای پیچیده، تحلیل ترافیکDNS ، دقت بالا از نقاط قوت این روش می باشد. پیچیدگی مدل، عدم تمرکز خاص بر پاسخ‌های ناموفق.DNS نقاط ضعف این روش می باشد.

Patel و همکاران [۲۶] از این مقاله از ترکیب چندین تکنیک ماشین لرنینگ برای تشخیص باتنت‌ها استفاده کرده و نشان می‌دهد که این ترکیب می‌تواند دقت تشخیص را بهبود بخشد. استفاده از ترکیب چندین تکنیک، استفاده از داده‌های واقعی و متنوع، چارچوب کارآمد از نقاط قوت این روش می باشد. پیچیدگی بیشتر، عدم تمرکز خاص بر پاسخ‌های ناموفقDNS نقاط ضعف این روش می باشد.

Choi و همکاران [۱۳]، [۱۴] و [۱۵] یک روش تشخیص بات نت مبتنی بر ناهنجاری ارائه کرده‌اند که با نظارت بر فعالیت‌های گروهی در ترافیک DNS، بات نت‌ها را در مراحل مختلف از چرخه حیات آن‌ها تشخیص می‌دهد. این فعالیت گروهی بر اساس پرس‌وجوهای DNS ارسال‌شده به‌صورت همزمان توسط بات های توزیع‌شده شکل می‌گیرد. در این روش، از ویژگی‌های متمایزکننده بین پرس‌وجوهای DNS بات نت برای تشخیص استفاده می‌شود. اگر بات‌های عضو یک بات نت تنها در مرحله شکل‌گیری از پرس‌وجوهای DNS استفاده کرده و یا از آدرس‌های IP به‌جای نام‌های دامنه استفاده کنند. روش فوق قادر به تشخیص آن بات نت نخواهد بود.

GU و همکاران [۱۶] ، [۱۷] یک روش مبتنی بر خوشه‌بندی برای تشخیص بات نت‌ها در مرحله حمله ارائه کرده‌اند. در این روش، ابتدا ترافیک ارتباطی مشابه و ترافیک بدخواهانه مشابه خوشه‌بندی‌شده و سپس یک همبستگی بین خوشه‌ای انجام می‌شود تا میزبان‌های دارای هر دو الگوی ارتباطی مشابه و الگوی فعالیت بدخواهانه مشابه شناسایی شوند. روش فوق به‌صورت غیر برخط عمل می‌کند که در سیستم‌های تشخیص بات نت یک ضعف عمده است.همچنین جدول زیر شامل برخی از مهم‌ترین کارهای مرتبط با تشخیص بات نت (Botnet) است که از روش‌های مختلف تحلیل پاسخ‌های ناموفق شبکه و استفاده از شبکه‌های عصبی استفاده کرده‌اند.

Arjun Singh, و [۲] Deepak Kumar, Suresh Reddy
orge Luis Reyes Ortiz, Daniel و [۳] Preeti Sharma
Roggen
[۴] و Anil Kumar, Praveen Kumar [۵] و Mirco]
Shashank Gupta, و [۶Marchetti, Michele Colajanni
] Harshal A. Patel, Kavita و [۷] Bharat Bhargava
و [۹] Sandeep Yadav, Ashwin L. Ganesh و [۸Sharma

] Wei Wang, Hui و [۱۰Nazanin]Zargari, Morteza Saebi
[۱۱Zeng, Dan Li روش‌های موثر برای تشخیص بات‌نت‌ها با استفاده از تحلیل ترافیک شبکه و تکنیک‌های هوش ارائه می دهند. از تحلیل‌های آماری و یادگیری ماشین برای شناسایی الگوهای غیرعادی در ترافیک شبکه استفاده کرده‌اند که می‌تواند نشان‌دهنده فعالیت بات‌نت باشد.

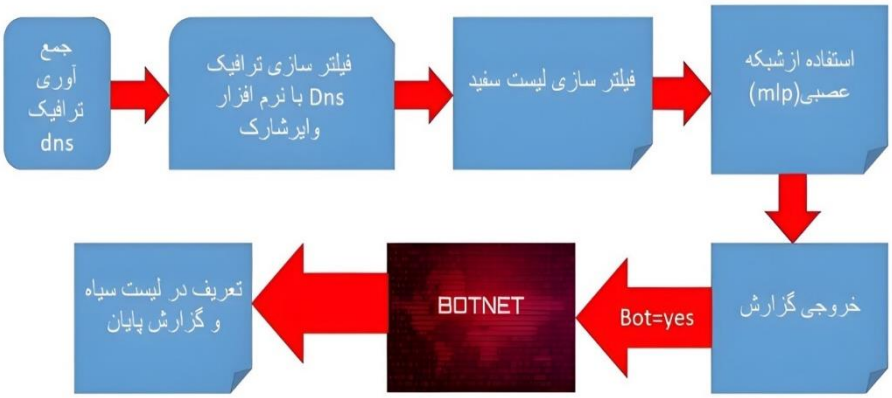
جدول ۱ روش های تشخیص بات‌نت‌ها با استفاده از تحلیل ترافیک شبکه و تکنیک‌های هوش

شماره	عنوان مقاله	نویسندگان	سال	روش پیشنهادی	نتایج کلیدی
۱	Effective Botnet Detection with Network Traffic Analysis and AI Techniques	Deepak Kumar, Suresh Reddy	2023	تحلیل ترافیک شبکه و تکنیک‌های هوش مصنوعی	تکنیک‌های هوش مصنوعی در کنار تحلیل ترافیک شبکه به بهبود دقت و سرعت تشخیص بات نت‌ها منجر شده است
۲	Hybrid Approach for Botnet Detection Using Machine Learning and Statistical Analysis	Arjun Singh, Preeti Sharma	2022	یادگیری ماشین و تحلیل آماری	ترکیب روش‌های آماری و یادگیری ماشین برای تشخیص بات نت‌ها نتایج مثبتی به همراه داشته است
۳	Anomaly-Based Botnet Detection Using Machine Learning and Flow Analysis	orge Luis Reyes Ortiz, Daniel Roggen	2021	تحلیل جریان شبکه و یادگیری ماشین	استفاده از تحلیل جریان شبکه و الگوریتم‌های یادگیری ماشین به تشخیص بات نت‌ها کمک می‌کند
۴	Automated Botnet Detection with Deep Learning Techniques	Anil Kumar, Praveen Kumar	2020	شبکه‌های عصبی عمیق	شبکه‌های عصبی عمیق توانسته‌اند به طور موثری بات نت‌ها را با دقت بالا تشخیص دهند
۵	Botnet Detection Using DNS Traffic Analysis and Machine Learning	Mirco Marchetti, Michele Colajanni	2019	تحلیل ترافیک DNS و یادگیری ماشین	استفاده از تحلیل ترافیک DNS و تکنیک‌های یادگیری ماشین باعث افزایش دقت تشخیص بات نت شد
۶	Detecting Botnets Using a Combined Approach of Network Traffic Analysis and Machine Learning	Shashank Gupta, Bharat Bhargava	2018	تحلیل ترافیک شبکه و ترکیب با یادگیری ماشین	ترکیب دو روش تحلیل ترافیک و یادگیری ماشین منجر به بهبود دقت و کاهش نرخ مثبت کاذب شد
۷	Real-Time Botnet Detection Using Machine Learning Techniques	Harshal A. Patel, Kavita Sharma	2017	تحلیل ترافیک شبکه و یادگیری ماشین در زمان واقعی	تشخیص بات نت در زمان واقعی با استفاده از مدل‌های یادگیری ماشین موثر و کارآمد است

۸	A Machine Learning Approach for Botnet Detection in Large-Scale Networks	Sandeep Yadav, Ashwin L. Ganesh	2015	یادگیری ماشین و تحلیل رفتار شبکه	مدل‌های یادگیری ماشین کارایی بالایی در تشخیص بات نت در شبکه‌های بزرگ دارند
۹	Detecting Botnets Using Network Traffic Behavior Analysis and Machine Learning Techniques	Nazanin Zargari, Morteza Saebi	2013	تحلیل ترافیک شبکه و یادگیری ماشین	ترکیب تحلیل ترافیک و الگوریتم‌های یادگیری ماشین منجر به افزایش دقت تشخیص بات نت شد
۱۰	Botnet Detection Based on Traffic Behavior Analysis and Artificial Neural Networks	Wei Wang, Hui Zeng, Dan Li	۲۰۱۰	تحلیل رفتار ترافیک و شبکه‌های عصبی مصنوعی	افزایش دقت تشخیص بات نت به کمک تحلیل رفتار ترافیک شبکه و مدل‌های شبکه عصبی

روش پیشنهادی برای تشخیص بات نت

تشخیص بات نت یک چالش پیچیده و مهم در حوزه امنیت سایبری است. بات نت‌ها مجموعه‌ای از دستگاه‌های متصل به اینترنت هستند که توسط مهاجمین کنترل می‌شوند و می‌توانند برای حملات سایبری مختلفی مانندDDoS ، ارسال هرزنامه و سرقت اطلاعات استفاده شوند. برای مقابله با این تهدیدات، شکل ۴ الگوی تشخیص بات نت پیشنهادی مبتنی بر از تحلیل پاسخ‌های ناموفق شبکه (NXDomain) ترافیک DNS و استفاده از شبکه عصبی پرسپترون چند لایه (MLP) را نشان می دهد. در شکل۴، معماری سیستم پیشنهادی ارائه‌شده است .روش پیشنهادی شامل شش مؤلفه اصلی هست که عبارت‌اند از جمع‌آوری ترافیک DNS فیلترسازی ترافیک NXDOMAIN، فیلترسازی فهرست سفید، استفاده از شبکه عصبی، تحلیل معیارهای سنجش و گزارش تشخیص بات نت.



شکل۴: الگوی تشخیص بات نت پیشنهادی مبتنی بر از تحلیل پاسخ‌های ناموفق شبکه (NXDomain) ترافیک DNS و استفاده از شبکه عصبی

جمع‌آوری ترافیکDNS:

سیستم پیشنهادی در سرویس‌دهنده DNS یا در لبه شبکه قرار می‌گیرد تا درخواست‌هایDNS ماشین‌های داخل شبکه و پاسخ‌های دریافتی را ثبت و نظارت نماید .واضح است فقط ترافیک DNS مدنظر است که درصد کمی از ترافیک کل شبکه هست .با توجه به فعالیت روزانه بات نت‌های مبتنی بر الگوریتم نام دامنه، فرض بر این است که این نوع از بات ها حداقل روزی یک‌بار اجرا می‌شوند؛ بنابراین حداکثر دوره زمانی برای جمع‌آوری ترافیک ۲۴ ساعت خواهد بود. با توجه به اینکهDNS یکی از رایج‌ترین پروتکل‌ها در شبکه است و برای کارکرد صحیح فعالیت‌های زیادی در شبکه‌ها ضروری است. به همین دلیل DNS برای مانیتورینگ، تشخیص و کاهش فعالیت بات نت‌ها بسیار مناسب است. در تشخیص مبتنی بر تحلیل ترافیک DNS به‌کل ترافیک شبکه نیاز نیست و فقط اطلاعات ترافیک DNS موردنیاز است و این باعث افزایش کارایی روشمان می‌گردد. ترافیک DNS حدود ۶ درصد از کل ترافیک شبکه است [۴] .

فیلترسازی فهرست سفید (Whitelist Filtering) برای تشخیص بات نت:

فیلترسازی فهرست سفید (Whitelist Filtering) یکی از موثرترین روش‌ها برای کاهش ترافیک مخرب و تشخیص فعالیت‌های غیرمجاز مانند بات نت‌ها در شبکه است. در این روش، تنها درخواست‌های DNS به دامنه‌های معتبر و شناخته‌شده که در فهرست سفید قرار دارند، مجاز به عبور از شبکه هستند. این رویکرد به طور قابل‌توجهی می‌تواند تعداد درخواست‌های DNS مشکوک و مخرب را کاهش دهد [۱۸]. در فیلترسازی فهرست سفید، فهرستی از نام‌های دامنه قابل‌اعتماد مثل google.com نگهداری می‌شود و درخواست و پاسخ‌های DNS مربوط به آن‌ها فیلتر می‌شود .بدین منظور، ابتدا ترافیک شبکه ضبط می‌شود. سپس بسته‌ها به/از سمت میزبان‌های موجود در فهرست سفید از این ترافیک حذف‌شده و سایر بسته‌های باقیمانده به‌عنوان ترافیک ورودی به مؤلفه بعدی داده می‌شوند .فیلتر سفید حجم ترافیک و درنتیجه حجم پردازش و نرخ خطای سیستم تشخیص را کاهش می‌دهد .برای ایجاد فهرست سفید، یک‌میلیون وب‌سایت برتر از Alex مورداستفاده قرار می‌گیرد .بدین دلیل که صد سایت پربازدید در اینترنت به‌احتمال‌زیاد به بات آلوده نیستند [۱۹] .

فیلترسازی ترافیک NXDomain :

در شبکه‌های بات، اعضای شبکه سعی در برقراری ارتباط با سرور فرماندهی و کنترل دارند تا دستورات حمله را دریافت نمایند، به همین دلیل شروع به فرستادن درخواست‌های رکورد A به سیستم DNS می‌نمایند. سیستم DNS نیز در پاسخ به این درخواست‌ها، با شرط وجود، رکورد A مربوطه را برمی‌گرداند و در غیراینصورت پاسخ ناموفق دریافت می‌شود .بدین ترتیب، برای تحلیل و استخراج اطلاعات، تنها ترافیک مربوط به سؤال/پاسخ رکوردهای A در ترافیک DNS بررسی می‌گردند. در فیلترسازی ترافیک NXDomain ، فقط درخواست‌هایی از رکورد A باقی خواهند ماند که دارای پاسخ‌های ناموفق یا NXDomainباشند و مابقی ترافیک DNS حذف خواهد شد؛ بنابراین بازهم حجم ترافیک ورودی به سیستم تشخیص کاهش خواهد یافت . همان‌طوری که اشاره گردید، یکی از ویژگی‌های کلیدی بات نت‌های مبتنی بر الگوریتم تولید نام دامنه، تولید روزانه نگاشت‌های ناموفق یا NXDomainها برای نام‌های دامنه‌ای است که وجود ندارند؛ بنابراین در میزبانی که به بات آلوده است تعداد NXDomain ها نسبت به میزبان‌های عادی به‌طور قابل‌توجهی بیشتر است NXDomain .ها غالباً به‌صورت گروهی تولید می‌شوند؛ بنابراین در ترافیک شبکه‌ای که آلوده به بات های موردنظر ما هستند، افزایش تعداد درخواست‌های رکورد A و در پی آن افزایش پاسخ‌های ناموفق یا NXDomain و درنهایت افزایش حجم ترافیک DNS نسبت به ترافیک کل شبکه اتفاق می‌افتد .در شکل ۳ درخواست‌های رکورد A و پاسخ‌های ناموفق در ترافیک DNS بات نت کراکن مشاهده می‌شود .این ترافیک از طریق اجرای کد بات کراکن بر روی یک میزبان متصل به اینترنت به‌دست‌آمده است.

No.	Time	Source	Destination	Protocol	Length	Info
6696	3111.05426	192.168.121.129	192.168.121.255	NBNS	92	Name query NB LXMYNOX.NET<00>
6697	3111.83053	192.168.121.129	192.168.121.2	DNS	78	Standard query 0x6238 A gfooaqf.dyndns.org
6698	3112.15882	192.168.121.2	192.168.121.129	DNS	129	Standard query response 0x6238 No such name
6699	3112.15921	192.168.121.129	192.168.121.2	DNS	90	Standard query 0xe3d0 A gfooaqf.dyndns.org.localdomain
6700	3112.50793	192.168.121.2	192.168.121.129	DNS	90	Standard query response 0xe3d0 No such name
6701	3112.63076	192.168.121.129	192.168.121.2	DNS	75	Standard query 0xd6c9 A egbmbdey.yi.org
6702	3112.85547	192.168.121.2	192.168.121.129	DNS	141	Standard query response 0xd6c9 No such name
6703	3112.85567	192.168.121.129	192.168.121.2	DNS	87	Standard query 0x956e A egbmbdey.yi.org.localdomain
6704	3112.89982	192.168.121.2	192.168.121.129	DNS	87	Standard query response 0x956e No such name

شکل ۵ :فعالیت بات نت کراکن و پاسخ‌هایNXDomain

انجام محاسبات و تحلیل معیارهای سنجش: از اطلاعات دریافتی از مؤلفه‌های قبلی و با انجام محاسباتی بر روی جدول نام دامنه برای هر IPیا میزبان معین، می‌تواند سه معیار تعریف نمود .معیارها عبارت‌اند از تعداد پاسخ‌های ناموفق یا NXDomain ها، تراکم درخواست‌های رکورد A و معیار گروه‌بندی .با بررسی میزان تحقق این معیارها، می‌توان درباره آلودگی به بات یا پاک بودن یک میزبان تصمیم گرفت .در ادامه به تشریح معیارها می‌پردازیم.

انجام محاسبات و تحلیل معیارهای سنجش:

الف-تعداد پاسخ‌های ناموفق: از جدول دامنه مربوط به هر IP یا میزبان معین، می‌توانیم تعداد کل NXDomain ها را در دوره زمانی T محاسبه نماییم .این تعداد را با n نشان می‌دهیم .دوره زمانی T با توجه به فعالیت روزانه بات نت‌های مبتنی بر تولید نام دامنه حداکثر برابر ۲۴ ساعت خواهد بود .در میزبانی که به بات آلوده است تعداد NXDomain ها نسبت به میزبان‌های عادی به‌طور قابل‌توجهی بیشتر است .اگر n بیش از یک حد آستانه باشد یکی از معیارهای آلودگی میزبان تحقق می‌یابد . حد آستانه در ادامه تعیین خواهد شد.

T : دوره زمانی برای ثبت و بررسی ترافیک(حداکثر ۲۴ ساعت)

n : تعداد کل NXDomain های محاسبه‌شده در دوره زمانی T

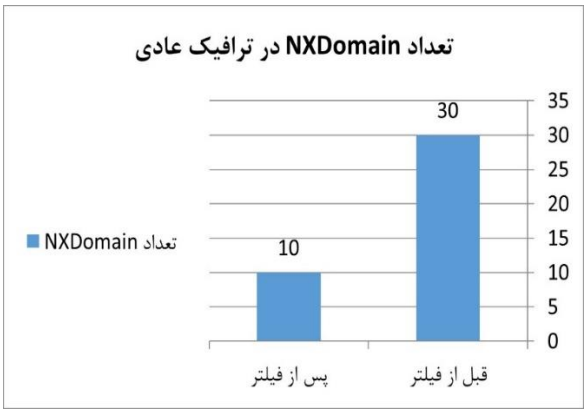
ب-تراکم درخواست‌های رکورد A : در ترافیک شبکه آلوده به بات های موردنظر، تعداد درخواست‌های رکورد A نسبت به ترافیک یک شبکه بی‌خطر بسیار بیشتر است .با توجه به اینکه زمان درخواست‌های رکورد A مربوط به هر دامنه در جدول دامنه مربوط به IP معین ثبت‌شده است، زمان درخواست هر رکورد برای نام دامنه i را با t_i نشان می‌دهیم .از t_i می‌توان متوسط فاصله زمانی مابین درخواست‌های رکورد A را طبق رابطه زیر به دست آورد:

$$p = \sum_{i=1}^{n-1} (t_{i+1} - t_i) / n - 1$$

از p برای سنجش تراکم تعداد درخواست‌های رکورد A در دوره زمانی T استفاده می‌شود .تراکم بیش از یک حد آستانه می‌تواند نشان‌دهنده وجود بات باشد.از اطلاعات و روابط فوق می‌توان درباره آلوده بودن یا عادی بودن نام‌های دامنه یک میزبان معین در دوره زمانی T تصمیم گرفت .بدین ترتیب که اگر معیارهای فوق در یک میزبان محقق شود آنگاه آن میزبان آلوده به بات تشخیص داده خواهد شد.

نتایج آزمایش:

فایل‌های اجرایی کانفیکر و کراکن، که از نوع بات نتهای مبتنی بر نام دامنه هستند از اینترنت دانلود و روی چند سیستم مجازی اجرا گردیدند .با استفاده از نرم افزار وایرشارک[۲۵] ، ترافیک بات نت‌های مذکور در هنگام فعالیت و به‌دفعات جمع‌آوری شد.ترافیک زمینه یا ترافیک بی‌خطر، با استفاده از نرم‌افزار وایرشارک و در محل سرور DNS شبکه دانشگاه،جمع‌آوری شد .همچنین در موارد متعدد و در ساعات مختلف، ترافیک میزبان‌های بی‌خطر متصل به اینترنت،به‌دست‌آمده و ذخیره شدند.در کلیه موارد فوق، ترافیک‌ها به‌صورت خام و بدون هیچ‌گونه پردازشی دربسته‌های pcap ذخیره شدند. تعداد کل NXDomainها را با n نشان می‌دهیم .محدوده زمانی نظارت بر ترافیک را با T نشان داده و مقدار آن را یک ساعت در نظر می‌گیریم. قبل و بعد از اعمال فیلترهای NXDomain و فهرست سفید در ترافیک عادی، تعداد NXDomain ها به‌دفعات برای یک میزبان متصل به اینترنت اندازه‌گیری شد و حداکثر آن در دوره زمانی T محاسبه شد .قبل از فیلتر n = ۳۰ و پس از فیلتر n = ۱۰ به دست آمد .این موضوع در نمودار شکل ۶ مشاهده می‌شود .



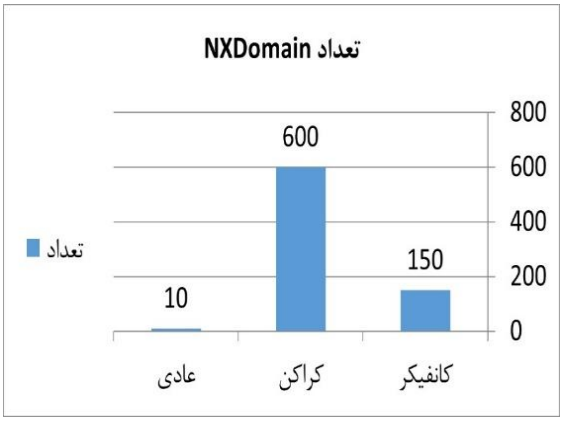
شکل۶ : تعداد NXDomain ترافیک عادی قبل و بعد از فیلترها

مواردی که فیلتر شده اند عبارت‌اند از درخواست‌های تکراری، درخواست‌های غیر از رکورد A یا درخواست‌های موجود در فهرست سفید بوده است. در جدول۲ مواردی از ترافیک DNS نشان داده‌شده است، این درخواست‌ها، غیر از رکورد A بوده‌اند و به همین دلیل فیلتر شده‌اند.

جدول۲ :پاسخ‌های NXDomain - فیلتر شده

Source	Destination	Protocol	Length	Info
192.168.1.2	192.168.1.1	DNS	84	Standard query 0x66be PTR 1.1.168.192.in-addr.arpa
192.168.1.1	192.168.1.2	DNS	133	Standard query response 0x66be No such name
192.168.1.2	192.168.1.1	DNS	92	Standard query 0x5d05 SRV _ldap._tcp.dc._msdcs.domain.name
192.168.1.1	192.168.1.2	DNS	155	Standard query response 0x5d05 No such name

در دوره یک‌ساعته T و پس از اعمال فیلترها، فعالیت باتنت کانفیکر، کراکن و ترافیک عادی با یکدیگر مقایسه شده است .مطابق نمودار شکل۷ ، تعداد NXDomain - ها در میزبان‌های آلوده بسیار بیشتر از میزبان‌های عادی است.



شکل۷ :نمودار تعدادNXDomain

حد آستانه‌ای به نام α تعریف نموده و میزبان‌هایی که بیش‌ازحد آستانه NXDomainدارند، در مرحله بعد گروه‌بندی می‌شوند و از بررسی سایر میزبان‌ها صرف‌نظر می‌شود .با استفاده از نتایج این بخش α =۱۰ خواهد بود .یعنی اگر پس از اعمال فیلتر NXDomain و فیلتر فهرست سفید، تعداد NXDomain های موجود در ترافیک، در محدوده زمانی یک ساعت، بیش از ۱۰ عدد باشد در مرحله بعد گروه‌بندی خواهند شد .در غیراینصورت از ادامه سایر مراحل صرف‌نظر نموده و آن میزبان در محدوده زمانی T غیر آلوده تشخیص داده می‌شود.

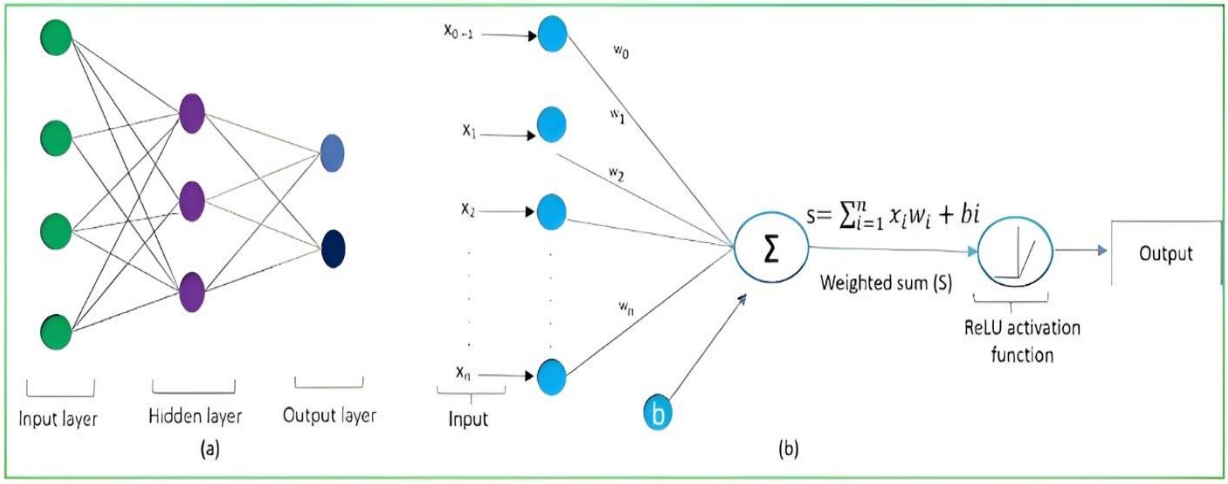
جدول۳ : متوسط فاصله زمانی بین درخواست‌های رکوردA در انواع ترافیک

نوع ترافیک	γ
کانفیکر	۸
کراکن	۳
عادی	>۱۰

مقدار γ = ۱۰را انتخاب می‌نماییم، .به این معنی که متوسط فاصله زمانی مابین درخواست‌های رکورد A درمواردی که کمتر از ۱۰ باشد ممکن است نشانه‌ای از آلودگی به بات باشد.

پیاده سازی شبکه عصبی پرسپترون چند لایه(MLP) :

ایده ما در حل تشخیص بات نت توسط شبکه عصبی پرسپترون چندلایه این است که متلب این ورودی‌ها را از فایل متنی خروجی وایرشارک گرفته و تحلیل می‌نماید که آیا شبکه مشکوک به بات است یا خیر؟ ما ابتدا باید با استفاده از ورودی‌ها و خروجی‌های به‌دست‌آمده از مراحل قبل که مطابق جدول و در یک فایل اکسل ذخیره هست این آموزش را به متلب می‌دهیم. آموزشات لازم توسط ورودی‌ها و هدف‌هایی که موردنظر ما هست انجام می‌گردد. ما در اینجا ۵ داده را به‌عنوان زمان درخواست در نظر گرفتیم برای هر شبکه‌ای که ترافیکش را گرفته‌ایم و متوسط زمان درخواست‌ها را با فرمول گفته شده در بالا به دست آوردیم که متلب این ورودی و خروجی‌ها را به‌طور خودکار از فایل اکسل دریافت و وزن‌های هر یال و بایاس‌های هر نرون را به دست می‌آورد. شکل ۸ نمونه ای از (a) معماری ساده یک شبکه عصبی مصنوعی و همچنین(b) تصویری از عملیات فعال سازی در شبکه عصبی مصنوعی با استفاده از تابع فعال سازیReLU را نشان می دهد.

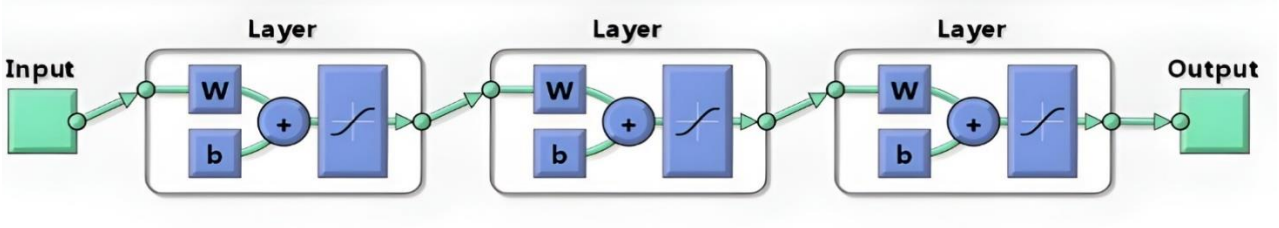


شکل ۸ نمونه ای از (الف) معماری و عملیات فعال سازی در شبکه عصبی [1]

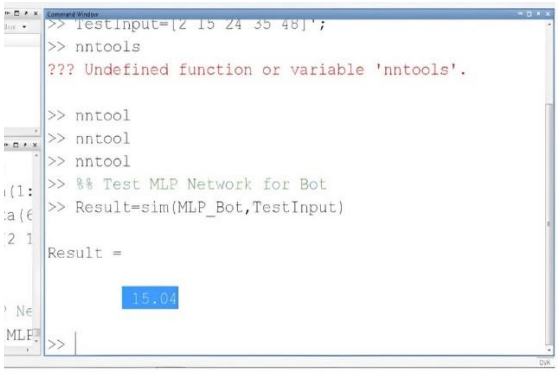
جدول ۴: ورودی و خروجی‌های شبکه عصبی پرسپترون چندلایه

	A	B	C	D	E	F	G
		RT1	RT2	RT3	RT4	RT5	Avg(RTi)
1	D1	1	9	23	54	98	24
2	D2	6	20	34	76	90	21
3	D3	2	30	80	90	120	24
4	D4	3	10	15	25	66	13
5	Conficker	4	12	22	30	36	9
6	Craker	1	4	5	8	13	3
7	D7	1	20	33	44	57	14
8	D8	10	15	57	90	112	25
9	D9	8	20	46	87	99	23
10	D10	1	14	29	39	59	15
11	D11	1	20	33	55	55	14
12	D12	10	15	57	90	99	22
13	D13	8	20	46	87	99	20
14	D14	1	14	29	39	59	15
15	D15	1	9	23	54	88	22
16	D16	6	20	34	76	90	21
17	D17	2	20	80	90	120	30
18	D18	3	10	15	25	45	11
19	D19	8	20	46	87	99	23
20	D20	1	14	29	39	59	15
21	D21	1	9	23	54	88	22
22	D22	6	20	34	76	90	21

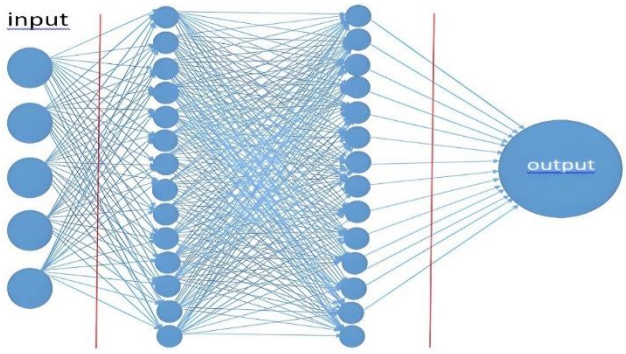
شکل‌های ۹ و ۱۰ نشان‌دهنده پیاده‌سازی مراحل شبکه عصبی ما هست. همان‌طور که مشاهده می‌کنید شبکه طراحی‌شده عصبی پرسپترون چندلایه ما شامل ۳ لایه ورودی، پنهان و خروجی هست؛ که هر لایه پنهان ما که در همان جعبه سیاه می‌باشند شامل ۱۴ نرون هست. ما از الگوریتم پس انتشار خطا در اینجا استفاده نمودیم این الگوریتم که در سال 1986 توسط روملهارت و مک کلیلاند پیشنهاد گردید، در شبکه‌های عصبی پیش‌سو مورداستفاده قرار می‌گیرد .پیش‌سو بودن به این معناست که نرون های مصنوعی در لایه‌های متوالی قرارگرفته‌اند و خروجی سیگنال خود را روبه‌جلو می‌فرستند .واژه پس انتشار نیز به معنای این است که خطاها به سمت عقب در شبکه تغذیه می‌شوند تا وزن ها را اصلاح کنند و پس‌ازآن، مجدداً ورودی مسیر پیش‌سوی خود تا خروجی را تکرار کند .روش پس انتشار خطا از روش‌های با سرپرست است به این مفهوم که نمونه‌های ورودی برچسب خورده اند و خروجی مورد انتظار هر یک از آن‌ها از پیش دانسته است . لذا خروجی شبکه با این خروجی‌های ایده آل مقایسه شده و خطای شبکه محاسبه می‌گردد .در این الگوریتم ابتدا فرض بر این است که وزن‌های شبکه به‌طور تصادفی انتخاب‌شده‌اند .در هر گام خروجی شبکه محاسبه‌شده و برحسب میزان اختلاف آن با خروجی مطلوب، وزن‌ها تصحیح می‌گردند تا درنهایت این خطا، مینیمم شود.



شکل۹: مدل ریاضی ساده‌شده شبکه عصبی برای تشخیص بات نت



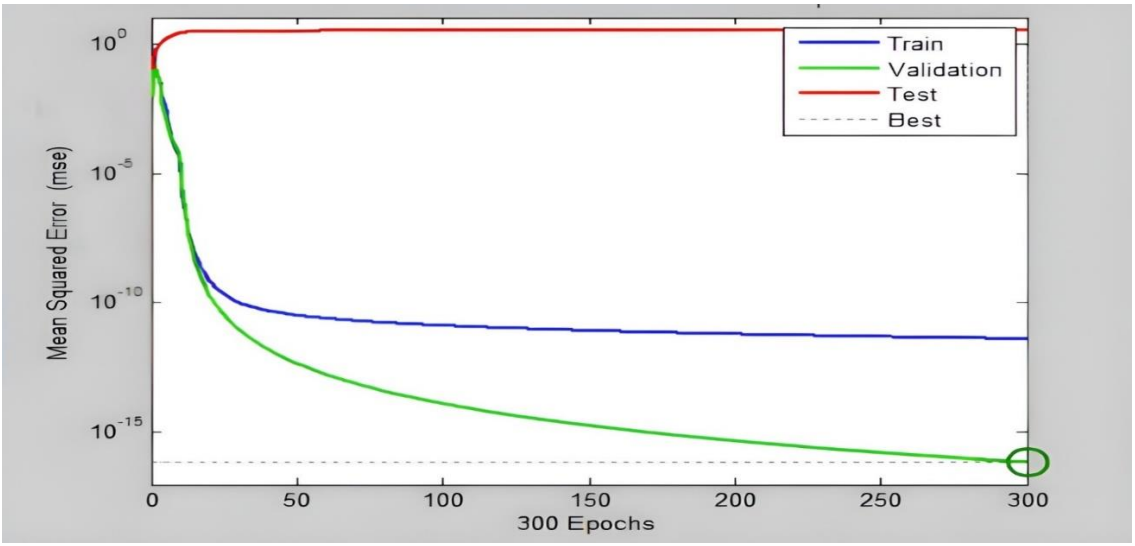
شکل ۱۱: مثالی از آزمون شبکه عصبی طراحی‌شده



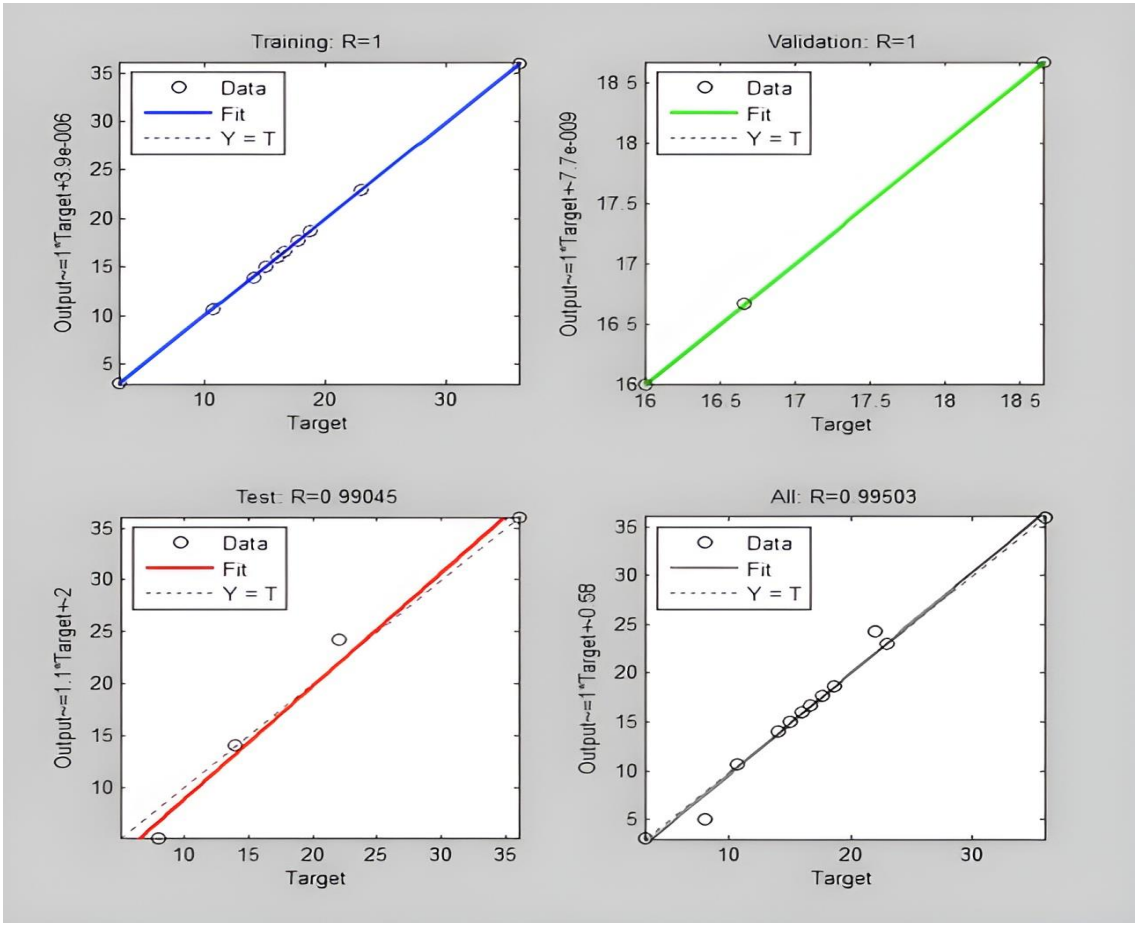
شکل ۱۰: شبکه عصبی پرسپترون چندلایه بات نت

پس از اینکه توسط متلب اعتبارسنجی‌های لازم انجام شد. می‌توانیم مطابق شکل ۱۱ آزمون‌هایمان را انجام بدهیم و به نتایج موردنظر که همان تشخیص بات نت هست به‌سادگی و بدون هیچ‌گونه تحلیلی برسیم.

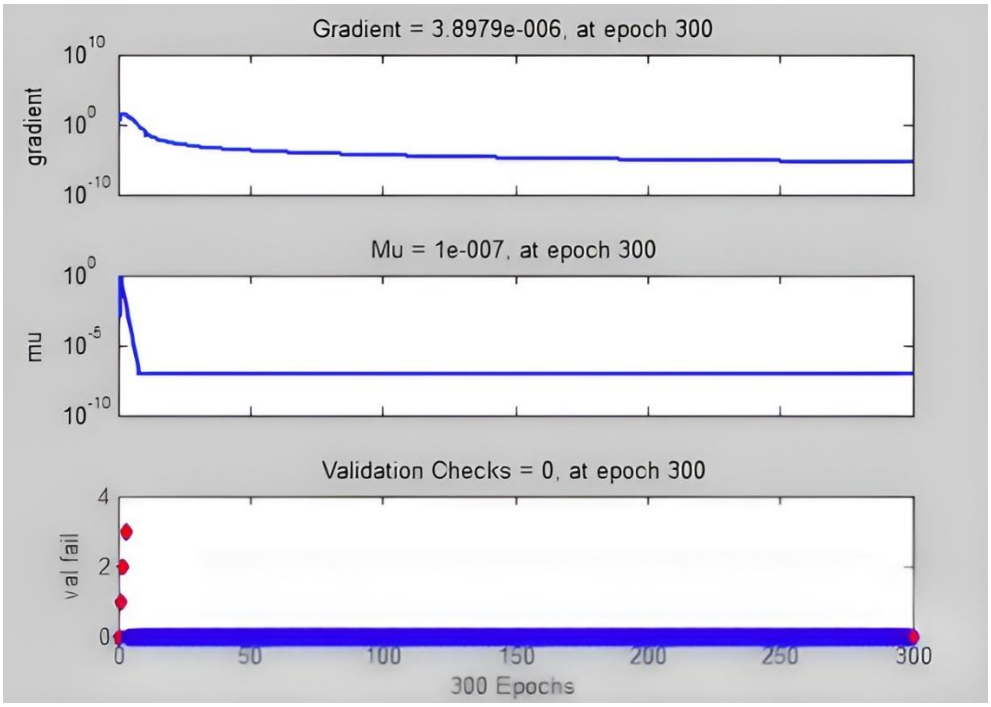
نمودار عملکرد که شامل نمودارهای آموزشی، آزمون و اعتبار سنجی هست در شکل‌های ۱۲, ۱۳ و ۱۴ نمایش داده‌شده است. که با توجه به اینکه در مرحله آموزش و اعتبار سنجی r=1 هست یعنی به‌طور کامل متلب آموزشات و اعتبار سنجی‌های لازم را در خصوص تشخیص بات نت دیده است. مرحله آزمون نیز r=0.99503 هست که این هم در حد ایده آل هست.



شکل ۱۲: تابع عملکرد و کار آیی شبکه عصبی طراحی‌شده



شکل ۱۳: تابع REGRESSION شبکه عصبی طراحی‌شده



شکل ۱۴: تابع TRAINING STATE شبکه عصبی طراحی‌شده

نتیجه گیری:

روش پیشنهادی ما ابتدا رفتارهای غیرعادی و پاسخهای ناموفق شبکه که ممکن است ناشی از فعالیت باتنت‌ها باشد را شناسایی می‌کند. سپس، با بهره‌گیری از شبکه‌های عصبی عمیق، الگوهای پنهان و پیچیده در این داده‌ها تحلیل می‌شوند. شبکه‌های عصبی با توانایی بالا در یادگیری الگوهای غیرخطی، ابزار قدرتمندی برای تشخیص دقیق و کارآمد باتنت‌ها ارائه می‌دهند. روش ما قابلیت تشخیص باتنت‌های شناخته‌شده و همچنین ناشناخته‌ای که از این روش استفاده می‌کنند را دارا هست. هدف ما در این مقاله، ارائه روشی نوآورانه برای تشخیص بات نت ها با استفاده از تحلیل پاسخ‌های ناموفق و شبکه عصبی است . در این روش تشخیص باتنت‌ها براساس پاسخ‌های ناموفق یا NXDomain در هر میزبان صورت می‌گیرد .این ویژگی باعث می‌شود که دقت تشخیص در شبکه‌های کوچک و متوسط افزایش یابد. نتایج آزمایش‌ها نشان‌دهنده دقت بالا و نرخ پایین مثبت کاذب مدل پیشنهادی در تشخیص باتنت‌ها است. این روش نه تنها قابلیت شناسایی سریع و موثر باتنت‌ها را دارد، بلکه می‌تواند به عنوان یک ابزار پیشگیرانه برای بهبود امنیت شبکه‌های کامپیوتری مورد استفاده قرار گیرد. این مطالعه نشان می‌دهد که تحلیل پاسخ‌های ناموفق شبکه با استفاده از شبکه‌های عصبی می‌تواند رویکردی مؤثر و عملی برای مقابله با تهدیدات امنیتی ناشی از باتنت‌ها باشد. استفاده از شبکه‌های عصبی برای آنالیز پاسخ‌های ناموفق DNS در تشخیص باتنت‌ها یک راهکار مؤثر و کارآمد است. این روش می‌تواند دقت تشخیص را افزایش دهد، الگوهای ناشناخته را شناسایی کند و قابلیت اطمینان سیستم‌های امنیتی را بهبود بخشد. با توجه به پیشرفت‌های اخیر در زمینه یادگیری عمیق و شبکه‌های عصبی، انتظار می‌رود که این روش‌ها در آینده نقش مهم‌تری در مقابله با تهدیدات امنیت سایبری ایفا کنند. پیاده‌سازی صحیح و رعایت امنیت و حریم خصوصی، کلید موفقیت این رویکرد در کاربردهای عملی است. ارائه رویکرد ترکیبی شبکه‌های عصبی مختلف مانندCNN ، RNNو LSTM و پیاده سازی رویکرد در محیط کاربردی اینترنت برای تشخیص بات نت از رویکردهای آتی پژوهش حاضر می باشد.

تعارض منافع

هیچ‌گونه تعارض منافع توسط نویسندگان بیان نشده است.

منابع:

[1] Maniriho P, Mahmood AN, Chowdhury MJM. Deep Learning Models for Detecting Malware Attacks. 2024.

[2] Kumar D, Reddy S. Effective Botnet Detection with Network Traffic Analysis and AI Techniques. J Netw Comput Appl. 2023.

[3] Singh A, Sharma P. Hybrid Approach for Botnet Detection Using Machine Learning and Statistical Analysis. J Cybersecurity. 2022.

[4] Reyes Ortiz JL, Roggen D. Anomaly-Based Botnet Detection Using Machine Learning and Flow Analysis. Comput Commun. 2021.

[5] Kumar A, Kumar P. Automated Botnet Detection with Deep Learning Techniques. J Inf Secur Appl. 2020.

[6] Wang W, Zeng H, Li D. Botnet Detection Based on Traffic Behavior Analysis and Artificial Neural Networks. IEEE Commun Mag. 2010.

[7] Zargari N, Saebi M. Detecting Botnets Using Network Traffic Behavior Analysis and Machine Learning Techniques. J Netw Comput Appl. 2013.

[8] Yadav S, Ganesh AL. A Machine Learning Approach for Botnet Detection in Large-Scale Networks. IEEE Trans Netw Serv Manag. 2015.

[9] Patel HA, Sharma K. Real-Time Botnet Detection Using Machine Learning Techniques. Comput Netw. 2017.

[10]Gupta S, Bhargava B. Detecting Botnets Using a Combined Approach of Network Traffic Analysis and Machine Learning. J Comput Secur. 2018.

[11]Marchetti M, Colajanni M. Botnet Detection Using DNS Traffic Analysis and Machine Learning. IEEE Trans Inf Forensics Secur. 2019.

[12]LeCun Y, Bengio Y, Hinton G. Deep learning. Nature. 2015;521(7553):436-444.

[13]Choi H, Lee H. Identifying botnets by capturing group activities in DNS traffic. 2011.

[14]Choi H, Lee H. Identifying botnets by capturing group activities in DNS traffic. Comput Netw. 2012;56:20-33.

[15]Choi H, et al. BotGAD: detecting botnets by capturing group activities in network traffic. In: Proceedings of the Fourth International ICST Conference on COMmunication System softWAre and middlewaRE; 2009; Dublin, Ireland.

[16]Gu G, et al. BotHunter: Detecting malware infection through ids-driven dialog correlation. In: Proceedings of 16th USENIX Security Symposium on USENIX Security Symposium; 2007; Boston, MA.

[17]Gu G, et al. Botminer: Clustering analysis of network traffic for protocol and structure independent Botnet detection. In: Proceedings of the 17th conference on Security symposium; 2008; San Jose, CA.

[18]Rahbarinia B, et al. Segugio: Efficient Behavior-Based Tracking of Malware-Control Domains in Large ISP Networks. In: NDSS Symposium; 2015.

[19]Alexa Top Global Sites. Available: http://www.alexa.com/topsites.

[20] Schoof R, Koning R. Detecting peer-to-peer botnets. University of Amsterdam, Technical report; 2007.

[21] Skoudis E, et al. Top Ten Cyber Security Menaces for 2008. SANS Institute; 2008.

[22] Cooke E, et al. The zombie roundup: understanding, detecting, and disrupting botnets; 2005.

[23]Park J. Acquiring Digital Evidence from Botnet Attacks: Procedures and Methods; 2011.

[24] Sharifnya R, Abadi M. A novel reputation system to detect DGA-based botnets. In: Computer and Knowledge Engineering (ICCKE), 2013 3th International eConference on; 2013. p. 417-423.

[25]Wireshark. Available: http://www.wireshark.org.

[26]Patel, P., & Modi, C. An Efficient Botnet Detection Framework Using Machine Learning Techniques; 2020.

[27]Lu, Y., Li, Z., & Zhang, C.DNS-based botnet detection using Long Short-Term Memory (LSTM) networks;2019.

[28]Wang, W., Xu, M., Huang, R., & Sun, Z.Botnet Detection Using Machine Learning Techniques; 2018.

[29] Antonakakis M, Perdisci R, Lee W, Vasiloglou N, Dagon D. Detecting Malware Domains at the Upper DNS Hierarchy. USENIX Security Symposium; 2010.

[30]Yu J, Li Z, Yan Q, Han J, Guan X. Network traffic characteristics analysis and anomaly detection on DNS. Comput Netw. 2017;117:87-99.

[31]Bilge L, Kirda E, Kruegel C, Balduzzi M. Exposure: Finding Malicious Domains Using Passive DNS Analysis. NDSS; 2011.