استفاده از یک روش خوشه‌بندی و محاسبه شهرت منفی هر میزبان به منظور تشخیص بات‌نت‌ها با استفاده از ترافیک DNS

رضا شریف‌نیای دیزبنی و آناهیتا منافی مورکانی

چکیده: امروزه بات‌نت‌ها به عنوان یکی از مهم‌ترین تهدیدها در برابر زیرساخت اینترنت شناخته می‌شوند. هر بات‌نت گروهی از میزبان‌های آلوده‌شده با کد مخرب یکسان است که توسط مهاجم و از طریق یک یا چند سرویس‌دهنده فرمان و کنترل از راه دور هدایت می‌شوند. از آنجایی‌که سرویس DNS یکی از مهم‌ترین سرویس‌ها در شبکه اینترنت است، مهاجمین از آن جهت مقاوم‌سازی بات‌نت خود استفاده می‌کنند. مهاجمین با استفاده از این سرویس دو تکنیک تغییر پی‌درپی آدرس IP و تغییر پی‌درپی نام دامنه را پیاده‌سازی می‌کنند. این تکنیک‌ها به مهاجم کمک می‌کنند تا مکان سرویس‌دهنده‌های فرمان و کنترل خود را به صورت پویا تغییر داده و از قرارگرفتن آدرس‌های آنها در فهرست‌های سیاه جلوگیری کنند. در این مقاله، یک روش خوشه‌بندی به همراه محاسبه شهرت منفی هر میزبان به منظور تشخیص برخط بات‌نت‌هایی پیشنهاد می‌شود که از سرویس DNS در مراحل مختلف از چرخه حیات خود استفاده می‌کنند. در روش پیشنهادی در پایان هر پنجره زمانی، ابتدا پرس و جوهای DNS با ویژگی‌های مشابه با استفاده از یک الگوریتم خوشه‌بندی انتخاب شده و در خوشه‌های جداگانه‌ای قرار می‌گیرند. سپس میزبان‌های مشکوک شناسایی شده و به ماتریس فعالیت‌های گروهی مشکوک اضافه می‌شوند. در نهایت، شهرت منفی میزبان‌های موجود در این ماتریس محاسبه شده و میزبان‌هایی که شهرت منفی بالایی دارند به عنوان میزبان‌های آلوده به بات گزارش می‌شوند. نتایج آزمایش‌های انجام‌شده نشان می‌دهد که روش پیشنهادی قادر است بات‌نت‌هایی را که از پرس و جوهای DNS در مراحل مختلف چرخه حیات خود استفاده می‌کنند با دقت بالا و نرخ هشدار نادرست پایین تشخیص دهد.

کلیدواژه: **تشخیص بات‌نت، محاسبه شهرت منفی، تغییر پی‌درپی آدرس IP، تغییر پی‌درپی نام دامنه، خوشه‌بندی پرس و جوی DNS.**

۱- مقدمه

با گسترش شبکه‌های کامپیوتری و ازدیاد حجم اطلاعات مورد مبادله در آنها، موضوع امنیت شبکه تبدیل به یک چالش بزرگ برای مدیران شبکه شده است. همزمان با پیشرفت فن‌آوری و ارائه خدمات نوین اینترنتی توسط شرکت‌های مختلف دولتی و خصوصی، مهاجمین نیز از عواملی چون ناآگاهی کاربران و آسیب‌پذیری‌های مختلف موجود در نرم‌افزارها سوء استفاده نموده و مشکلاتی را برای کاربران ایجاد کرده‌اند. امروزه امنیت اینترنت با یک تحول و تکامل از انواع حملات مواجه شده است. همواره تکنیک‌های پیچیده و متفاوت زیادی توسط مهاجمین در بدافزارها استفاده می‌شود تا بتوانند از شناخته‌شدن توسط سیستم‌های تشخیص نفوذ جلوگیری کنند [۱].

امروزه بات‌نت‌ها به عنوان یکی از مخرب‌ترین بدافزارها در مقابل زیرساخت اینترنت هستند که می‌توانند از تمام روش‌های موجود در بدافزارها برای پنهان‌سازی سرویس‌دهنده فرمان و کنترل (C & C)[1] خود استفاده کنند. هر بات‌نت شامل گروهی از میزبان‌های آلوده به کد مخرب یکسان است که توسط مهاجم و از طریق یک یا چند سرویس‌دهنده فرمان و کنترل از راه دور هدایت می‌شوند. مهاجم از این میزبان‌ها برای انجام فعالیت‌های غیر قانونی از قبیل ارسال هرزنامه[2]، حمله‌های جلوگیری از سرویس توزیعی، سرقت اطلاعات محرمانه[3] و غیره به نفع خود سوء استفاده می‌کند و این در حالی است که معمولاً هویت وی مخفی می‌ماند [۲]. مدیران بات[4] به این نتیجه رسیده‌اند که با استفاده از دو تکنیک تغییر پی‌درپی آدرس IP[5] و تغییر پی‌درپی نام دامنه[6]، از اتصال بات‌های زیاد به یک آدرس و در نتیجه کشف این بات‌ها و از بین رفتن بات‌نت جلوگیری کنند. تکنیک تغییر پی‌درپی آدرس IP تکنیکی است که به صورت پویا آدرس‌های IP ثبت‌شده برای یک نام دامنه را تغییر می‌دهد. در تکنیک تغییر پی‌درپی نام دامنه، نام‌های دامنه‌ای که به یک آدرس IP نگاشت می‌شوند به صورت دوره‌ای عوض می‌شوند. این روش‌ها با نسبت‌دادن طول عمر کوتاه به پرس و جوهای DNS و استفاده از الگوریتم‌های زمان‌بندی نوبت گردشی[7] قابل اجرا هستند.

بر خلاف دیگر بدافزارها که به طور مستقل کار می‌کنند، یک بات‌نت به یک زیرساخت ارتباطی نیاز دارد تا مدیر بات بتواند از طریق آن فرامین خود را برای بات‌ها ارسال کرده و پاسخ آنها را دریافت کند. این زیرساخت ارتباطی با نام کانال‌های فرمان و کنترل شناخته می‌شود. در این مقاله، روشی برای تشخیص برخط بات‌نت‌ها پیشنهاد می‌شود که از سابقه فعالیت‌های گروهی مشکوک در ترافیک DNS برای محاسبه شهرت منفی میزبان‌های آلوده استفاده می‌کند. استفاده از ترافیک DNS دو مزیت عمده دارد: ۱) پرس و جوهای DNS حجم محدودی از ترافیک شبکه را تشکیل داده و بنابراین استفاده از ترافیک DNS باعث کاهش هزینه فرایند تشخیص می‌شود و ۲) با توجه به این که پرس و جوهای DNS در مراحل اولیه چرخه حیات بات‌نت‌ها ارسال می‌شوند، میزبان‌های آلوده قبل از انجام هر گونه فعالیت بدخواهانه شناسایی می‌شوند.

در بخش ۲ تحقیق‌های پیشین در زمینه تشخیص بات‌نت‌ها با استفاده از ترافیک DNS بررسی شده و در بخش ۳ روش پیشنهادی برای

این مقاله در تاریخ ۳۱ اردیبهشت ماه ۱۳۹۳ دریافت و در تاریخ ۹ تیر ماه ۱۳۹۴ بازنگری شد.

رضا شریف‌نیای دیزبنی، گروه مهندسی کامپیوتر، دانشکده مهندسی برق و کامپیوتر، دانشگاه تربیت مدرس، تهران، (email: Reza.sharifnyay@modares.ac.ir).

آناهیتا منافی مورکانی، گروه مهندسی کامپیوتر، دانشکده مهندسی برق و کامپیوتر، دانشگاه تربیت مدرس، تهران، (email: Anahita.manafi@modares.ac.ir).

1. Command and Control Server
2. Spaming
3. Information Leakage
4. Botmasters
5. IP Flux
6. Domain Flux
7. Round Robin Algorithms

تشخیص برخط بات‌نت‌ها معرفی می‌شود. در بخش ۴ نتایج آزمایش‌های انجام‌شده برای ارزیابی کارایی روش پیشنهادی ارائه می‌شود و در بخش ۵ نتیجه‌گیری به عمل می‌آید.

۲- تحقیق‌های پیشین

تا کنون روش‌های زیادی برای شناسایی بات‌نت‌ها با استفاده از ترافیک DNS ارائه شده‌اند که به مرور زمان و با توجه به تغییرات و پیشرفت سریع نحوه عملکرد این دسته از بات‌نت‌ها، هیچ کدام نتوانسته‌اند روشی جامع را معرفی نمایند. در این بخش، تحقیق‌های انجام‌شده در این زمینه مورد بررسی قرار گرفته و ایده اصلی روش‌های معرفی‌شده بیان می‌شود.

Holz و همکاران [۲] روشی برای شناسایی شبکه‌های سرویس تغییرات پی‌درپی آدرس IP پیشنهاد کردند. آنها با مشاهده رفتارهای موجود در شبکه‌های تغییر پی‌درپی آدرس IP، یک تابع امتیازدهی به نام‌های دامنه را پیشنهاد دادند که مقدار این امتیاز احتمال متعلق‌بودن نام دامنه به شبکه تغییر پی‌درپی آدرس IP را مشخص می‌کند. تابع امتیازدهی آنها با استفاده از یک تابع رگرسیون خطی و سه ویژگی زیر طراحی شده است: تعداد رکوردهای آدرس یکتا[1]، تعداد سیستم‌های خودمختار[2] مجزا و تعداد رکوردهای سرور نام دامنه مجزا. با وجود این وزن‌های تابع رگرسیون خطی در این روش وابسته به ویژگی‌های شبکه‌ای دارند که این روش در آن پیاده می‌شود.

Yadav و همکاران [۳] روشی مبتنی بر شناسایی نام‌های دامنه الگوریتمی برای تشخیص بات‌نت‌های نسل جدید ارائه کرده‌اند که از توزیع کاراکترهای حرفی- عددی در پرس و جوهای DNS استفاده می‌کند. این روش به تعداد زیاد پرس و جوهای DNS وابسته بوده و به دلیل عدم توجه به سابقه فعالیت‌های گروهی مشکوک در میزبان‌های شبکه از نرخ هشدار نادرست بالایی برخوردار است. همچنین معیارهای آنها تنها توزیع دوتایی‌هایی را در نظر می‌گیرند که در هر دو دسته نام‌های دامنه قانونی و نام‌های دامنه مورد بررسی قرار دارند. بنابراین یک مدیر بات به سادگی می‌تواند نام‌های دامنه‌ای را ایجاد کند که تفاوت زیادی با نام‌های دامنه اصلی داشته باشند، اما مقدار واگرایی کمی را با استفاده از معیارهای آنها دارند. آنها در [۴] روش دیگری ارائه کرده‌اند که از شکست‌ها در پرس و جوهای DNS برای سرعت‌بخشیدن به فرایند تشخیص استفاده می‌کند.

Kruegel و همکاران [۵] روشی به نام EXPOSURE ارائه کردند که از پانزده ویژگی به منظور دسته‌بندی نام‌های دامنه استفاده می‌کند. این ویژگی‌ها برای شناسایی جنبه‌های متفاوت رفتارهای مخرب نام‌های دامنه استفاده می‌شوند. پس از استخراج این ویژگی‌ها، EXPOSURE از الگوریتم درخت تصمیم J۴۸ به منظور دسته‌بندی نام‌های دامنه استفاده کرده تا مشخص کند یک نام دامنه بر اساس ویژگی‌هایش مخرب است یا خیر. EXPOSURE به دلیل عدم توجه به سابقه فعالیت‌های گروهی مشکوک در میزبان‌های شبکه از نرخ هشدار نادرست بالایی برخوردار است.

Antonakakis و همکاران [۶] سیستمی به نام Pleiades پیشنهاد کردند که ترافیک DNS محلی را تحت کنترل قرار می‌دهد. سیستم Pleiades درخواست‌های ناموفق DNS را که به تعداد زیاد و با مشخصه‌های یکسان توسط تعدادی کامپیوتر خاص و ثابت در شبکه ارسال می شوند، به عنوان نشانه و علامتی از فعالیت یک شبکه مخرب بات‌نت تلقی می‌کند. در صورتی که یک میزبان آلوده درخواست‌های ناموفق DNS نداشته باشد، Pleiades قادر به شناسایی آن میزبان نیست.

Choi و همکاران [۷] یک روش برخط غیر نظارتی را برای تشخیص بات‌نت‌ها با نام BotGAD پیشنهاد کرده‌اند. آنها معیاری برای تشخیص بات‌نت‌ها با نظارت بر فعالیت‌های گروهی در ترافیک DNS ارائه کرده‌اند. در واقع فعالیت گروهی بات‌ها در ترافیک DNS به ویژگی‌هایی گفته می‌شود که این ترافیک را از ترافیک عادی متمایز می‌سازد. در این روش، نرخ تشخیص تا حد زیادی وابسته به انتخاب اندازه مناسب برای پنجره‌های زمانی است و به دلیل عدم توجه به سابقه فعالیت‌های گروهی مشکوک میزبان‌ها از کارایی مناسبی برای تشخیص بات‌نت‌های نسل جدید برخوردار نیست.

Davuth و همکاران [۸] روشی ارائه کردند که نام‌های دامنه با استفاده از دسته‌بند SVM دسته‌بندی می‌شوند. آنها با استفاده از دوتایی‌ها[3]، ویژگی‌هایی را از نام‌های دامنه استخراج و سپس نام‌های دامنه را بر اساس این ویژگی‌ها دسته‌بندی می‌کنند. این روش به دلیل عدم توجه به ویژگی‌های ذاتی بات‌نت‌ها (از قبیل فعالیت‌های گروهی) از کارایی مناسبی برای تشخیص بات‌نت‌های نسل جدید برخوردار نیست.

۳- روش پیشنهادی

در این بخش، ابتدا برخی از مفاهیم مورد استفاده در این مقاله تعریف شده و سپس مراحل اصلی روش پیشنهادی شرح داده می‌شوند.

۳-۱ تعاریف اولیه

به منظور درک بهتر بات‌نت‌هایی که از سرویس DNS سوء استفاده می‌کنند، نیازمند آشنایی با اصطلاحات به کار رفته در این حوزه می‌باشیم. در ادامه مفاهیم اصلی مربوط به این دسته از بات‌نت‌ها به طور کامل بیان می‌شوند.

در بات‌نت‌های مبتنی بر تغییر پی‌درپی نام دامنه، مهاجمین با استفاده از الگوریتم‌های تولید نام دامنه مکان سرویس‌دهندگان فرمان و کنترل خود را به صورت دوره‌ای تغییر داده تا از قرارگرفتن آدرس‌های آنها در فهرست‌های سیاه جلوگیری کنند.

تعریف ۱ (نام دامنه): نام منحصر به فردی است که برای شناسایی یک آدرس اینترنتی مورد استفاده قرار می‌گیرد. هر نام دامنه شامل یک یا چند قسمت است که با نقطه (.) از هم جدا می‌شوند. به هر یک از این قسمت‌ها یک توکن گفته می‌شود.

تعریف ۲ (تغییر پی‌درپی نام دامنه): روشی که با استفاده از آن تعداد زیادی نام دامنه توسط پرس و جوهای DNS به آدرس IP یکسانی نگاشت می‌شوند.

مدیران بات جهت پیاده‌سازی تکنیک تغییر پی‌درپی نام دامنه دو روش متفاوت استفاده از زیردامنه‌های تصادفی[4] و الگوریتم‌های تولید نام دامنه[5] را به کار می‌گیرند. همچنین به منظور عدم شناسایی آدرس IP سرویس‌دهنده فرمان و کنترل از تکنیک تغییر پی‌درپی آدرس IP استفاده می‌کنند.

1. Unique
2. Autonomous System
3. Bigrams
4. Domain Wildcarding
5. Domain Generation Algorithms

جدول ۱: ویژگی‌های استفاده‌شده در روش پیشنهادی.

نوع ویژگی	نام ویژگی
ویژگی‌های مربوط به توکن‌ها	– تعداد توکن‌ها – ماکسیمم اندازه توکن‌ها
ویژگی‌های مربوط به توزیع کاراکترهای حرفی– عددی	– معیار واگرایی J-S – ضریب همبستگی SRCC
ویژگی‌های مربوط به اطلاعات پاسخ پرس و جوهای DNS	– تعداد آدرس‌های IP نگاشت‌شده – تعداد شبکه‌های خودمختار متفاوت – طول عمر پرس و جوی DNS

تعریف ۳ (زیردامنه‌های تصادفی): روشی است که به مدیران بات‌نت اجازه می‌دهد تا تمام زیردامنه‌های تصادفی ایجادشده برای یک نام دامنه ثبت‌شده را به یک آدرس IP نگاشت کنند. به عنوان مثال، هر دو پرس و جوی sub1.malicious.com و sub2.malicious.com به آدرس IP پرس و جوی malicious.com نگاشت می‌شوند. این روش با قراردادن کاراکتر * در سمت چپ یک نام دامنه ایجاد می‌شود.

تعریف ٤ (الگوریتم تولید نام دامنه): یک الگوریتم از پیش تعریف شده در کد بات که فهرستی از نام‌های دامنه سرویس‌دهنده‌های فرمان و کنترل را به صورت پویا تولید می‌کند. هر نام دامنه در این فهرست، یک نام دامنه الگوریتمی نامیده می‌شود.

تعریف ٥ (تغییر پی‌درپی آدرس IP): تکنیکی که با استفاده از آن تعداد زیادی آدرس IP به یک پرس و جوی DNS اختصاص داده می‌شوند.

در روش پیشنهادی برای نگهداری سابقه فعالیت‌های گروهی مشکوک در ترافیک DNS و محاسبه شهرت منفی میزبان‌های آلوده از ماتریس فعالیت‌های گروهی مشکوک استفاده می‌شود.

تعریف ٦ (فعالیت گروهی[1]): ارسال تعدادی پرس و جوی DNS یک فعالیت گروهی نامیده می‌شود اگر نام‌های دامنه در این پرس و جوها به آدرس یکسانی نگاشت شده یا حداقل بخشی از نام‌های دامنه آنها (توکن‌ها) یکسان باشد. قابل ذکر است که در یک فعالیت گروهی حداقل دو میزبان باید مشارکت داشته باشند.

تعریف ۷ (فعالیت گروهی مشکوک): یک فعالیت گروهی مشکوک نامیده می‌شود اگر نام‌های دامنه در پرس و جوهای DNS به صورت الگوریتمی ایجاد شده باشند.

تعریف ۸ (ماتریس فعالیت‌های گروهی مشکوک): یک ماتریس دودویی که مشخص می‌کند هر میزبان در کدام پنجره‌های زمانی حداقل در یک فعالیت گروهی مشکوک مشارکت داشته است. این ماتریس با $G_{n\times m}$ نمایش داده می‌شود که n تعداد کل میزبان‌های شبکه و m تعداد پنجره‌های زمانی قبلی است. هر عنصر $g_{ik} \in G$ در صورتی برابر با ۱ است که میزبان h_i در kامین پنجره زمانی قبلی حداقل در یک فعالیت گروهی مشکوک مشارکت داشته باشد.

تعریف ۹ (شهرت منفی[2]): برآورد عمومی از میزان فعالیت‌های مشکوک هر میزبان شبکه است. شهرت منفی هر میزبان امتیازی بین ۰ و ۱ است که بر اساس سابقه فعالیت‌های مشکوک آن میزبان محاسبه می‌شود. در سیستم‌های مبتنی بر شهرت از فعالیت‌های گذشته هر میزبان برای پیش‌بینی فعالیت‌های آینده آن استفاده می‌شود [۹].

1. Group Activity
2. Negative Reputation

۳-۲ مراحل اصلی روش پیشنهادی

همان طور که پیش از این گفته شد، در روش پیشنهادی از ترافیک DNS جهت شناسایی میزبان‌های آلوده به بات‌نت استفاده می‌شود. بنابراین اولین گام در روش پیشنهادی جداسازی ترافیک DNS از ترافیک عادی شبکه است.

روش پیشنهادی شامل چهار مرحله اصلی است که در ادامه به طور کامل تشریح می‌شوند: ۱) فیلترسازی فهرست سفید، ۲) خوشه‌بندی پرس و جوهای DNS، ۳) شناسایی خوشه‌های مشکوک و ۴) محاسبه شهرت منفی میزبان‌ها.

۳-۲-۱ فیلترسازی فهرست سفید

در پایان هر پنجره زمانی، ترافیک DNS با یک فهرست سفید از نام‌های دامنه قانونی (به عنوان مثال، نام‌های دامنه موتورهای جستجو) فیلتر می‌شود. اندازه هر پنجره زمانی مقداری ثابت است که توسط کاربر تعیین می‌شود. عملیات فیلترسازی فهرست سفید باعث جلوگیری از انجام محاسبات اضافی بر روی پرس و جوهایی می‌شود که از نام‌های دامنه موجود در این فهرست استفاده می‌کنند. برای ایجاد فهرست سفید از نام‌های دامنه پنجاه وب‌سایت برتر گزارش‌شده توسط Alexa [۱۰] استفاده شده است.

۳-۲-۲ خوشه‌بندی پرس و جوهای DNS

بات‌های عضو یک بات‌نت به دلیل استفاده از کدهای دودویی یکسان، رفتار مشابهی را در دوره‌های زمانی نزدیک به هم از خود نشان می‌دهند. این نوع رفتار بات‌نت‌ها در نقطه مقابل رفتار میزبانی‌هایی است که توسط کاربران انسانی کنترل می‌شوند [۱۱]. بنابراین در صورت خوشه‌بندی، پرس و جوهای DNS ارسال‌شده توسط میزبان‌های آلوده در یک خوشه قرار می‌گیرند. در این مقاله به منظور خوشه‌بندی پرس و جوهای DNS از الگوریتم خوشه‌بندی با شعاع ثابت و ۷ ویژگی متفاوت در پرس و جوهای DNS استفاده شده است. این ویژگی‌ها در سه دسته مختلف بررسی می‌شوند تا درک آنها آسان‌تر شود: الف) ویژگی‌های مربوط به توکن‌های[3] پرس و جوهای DNS، ب) ویژگی‌های مربوط به توزیع کاراکترهای حرفی– عددی نام‌های دامنه پرس و جوهای DNS[4] و ج) ویژگی‌های به دست آمده از اطلاعات مربوط به پاسخ پرس و جوهای DNS[5]. جدول ۱ ویژگی‌های استفاده‌شده برای خوشه‌بندی پرس و جوهای DNS را نشان می‌دهد.

الف) ویژگی‌های مربوط به توکن‌ها

نام‌های دامنه‌ای که توسط بات‌نت‌های مبتنی بر تغییر پی‌درپی آدرس IP و تغییر پی‌درپی نام دامنه ایجاد می‌شوند الگوهای متفاوتی نسبت به نام‌های دامنه قانونی دارند. به عنوان مثال، بات‌نت‌هایی که از الگوریتم تولید نام دامنه استفاده می‌کنند، نام‌های دامنه با طول و تعداد توکن یکسان ایجاد می‌کنند. تعداد توکن‌ها و ماکسیمم اندازه توکن‌ها ویژگی‌هایی هستند که از توکن‌های موجود نام‌های دامنه محاسبه شده‌اند [۵].

ب) ویژگی‌های مربوط به توزیع کاراکترهای حرفی– عددی

این دسته از ویژگی‌ها نام‌های دامنه پرس و جوها را بررسی کرده و

3. Token Features
4. DNS Lexicology
5. DNS Answer Information

برای شناسایی بات‌نت‌های مبتنی بر تغییر پی‌درپی نام دامنه مؤثر هستند. در روش پیشنهادی معیارهای مختلفی برای محاسبه توزیع کاراکترهای حرفی- عددی نام‌های دامنه پرس و جوهای DNS آزمایش شده‌اند. اما دو ویژگی معیار واگرایی J-S و ضریب همبستگی SRCC در موارد مختلف نتایج بهتری را حاصل کرده‌اند که در ادامه نحوه محاسبه این دو ویژگی به طور کامل شرح داده می‌شود.

ب- ۱) معیار واگرایی J-S

در نظریه احتمال از معیار واگرایی J-S به عنوان یک معیار متقارن برای اندازه‌گیری فاصله بین دو توزیع احتمال متفاوت استفاده می‌شود [۱۲]. فرض کنید $H(P)$ آنتروپی شانون[1] توزیع احتمال P باشد

$$H(P) = -\sum_{i=1}^{l} P(i) \cdot \log P(i) \qquad (۱)$$

l مقادیر ممکن برای یک متغیر تصادفی گسسته است. برای دو توزیع احتمال تصادفی P و Q، معیار واگرایی J-S با $D_{JS}(P,Q)$ نمایش داده شده و به صورت زیر تعریف می‌شود

$$D_{JS}(P,Q) = H(\frac{1}{2}(P+Q)) - \frac{1}{2}(H(P)+H(Q)) \qquad (۲)$$

که در آن P توزیع پایه و Q توزیع آزمون است. ابتدا توزیع دوتایی‌ها در هر پرس و جو به منظور به دست آوردن توزیع آزمون برای پرس و جوهای DNS محاسبه می‌شود. به هر زوج کاراکتر حرفی- عددی متوالی دوتایی گفته می‌شود. به‌عنوان مثال در رشته "bot" زوج کاراکترهای "bo" و "ot" دوتایی‌ها هستند. سپس معیار واگرایی J-S با استفاده از توزیع‌های پایه و آزمون برای همه پرس و جوهای DNS در توزیع آزمون محاسبه شده و از مقادیر به دست آمده به عنوان مقدار ویژگی معیار واگرایی J-S هر پرس و جو استفاده می‌شود. برای محاسبه توزیع پایه از یک میلیون وب‌سایت برتر گزارش‌شده توسط Alexa [۱۰] استفاده شده است.

ب- ۲) ضریب همبستگی SRCC

ضریب همبستگی SRCC وابستگی آماری بین دو متغیر با مقادیر رتبه‌بندی شده را نشان داده و با ρ نمایش داده می‌شود [۱۳]. در روش پیشنهادی از این معیار به عنوان یک ویژگی برای محاسبه میزان همبستگی بین تکرارهای رتبه‌بندی شده لیستی از دوتایی‌ها استفاده می‌شود. رتبه تکرار دوتایی‌ها در نام‌های دامنه قانونی با استفاده از نام‌های دامنه یک میلیون وب‌سایت برتر گزارش‌شده توسط Alexa [۱۰] محاسبه شده که به آن رتبه پایه گفته می‌شود. برای تعیین میزان تصادفی‌بودن پرس و جوهای DNS، ابتدا رتبه تکرار هر دوتایی موجود در هر پرس و جو محاسبه شده و با استفاده از (۳) مقدار ضریب همبستگی SRCC بین این رتبه و رتبه پایه محاسبه می‌شود

$$\rho = \left| 1 - \frac{6}{n(n^2-1)} \sum_{i=1}^{n} d_i^2 \right| \qquad (۳)$$

که در آن n تعداد دوتایی‌ها و d_i اختلاف بین دو رتبه دوتایی مورد بررسی i می‌باشد. مقدار همبستگی ρ بین ۰ و ۱ تغییر می‌کند که مقادیر نزدیک به ۰ نشان‌دهنده عدم وجود همبستگی و مقادیر نزدیک به ۱ نشان‌دهنده وابستگی بیشتر بین رتبه‌ها است.

ج) ویژگی‌های مربوط به اطلاعات پاسخ پرس و جوهای DNS

مدیران بات به‌طور معمول از نام‌های دامنه‌ای استفاده می‌کنند که پرس و جوهای DNS آنها به آدرس‌های IP متفاوتی نگاشت شده و در شبکه‌های خودمختار[2] متفاوتی قرار دارند. بنابراین در روش پیشنهادی سه ویژگی مربوط به اطلاعات پاسخ پرس و جوهای DNS محاسبه شده است: ۱) تعداد آدرس‌های IP نگاشت‌شده برای هر پرس و جوی DNS، ۲) تعداد شبکه‌های خودمختار متفاوت و ۳) طول عمر پرس و جوهای DNS. این دسته از ویژگی‌ها برای شناسایی بات‌نت‌هایی مؤثر هستند که از تکنیک تغییر پی‌درپی آدرس IP استفاده می‌کنند. مهاجمین با دادن مقدار کم به طول عمر پرس و جوهای DNS، علاوه بر دسترس‌پذیری بالا می‌توانند مقاومت بیشتر بات‌نت خود را در مقابل سیستم‌های تشخیص نفوذ تضمین کنند. طول عمر یک پرس و جوی DNS نشان می‌دهد که این پرس و جو چه مدت زمانی در حافظه کش در دسترس باشد [۷].

با استفاده از این سه دسته ویژگی‌ها و الگوریتم خوشه‌بندی با شعاع ثابت، پرس و جوهای DNS خوشه‌بندی شده و سپس خوشه‌هایی که میزان شباهت پرس و جوهای DNS در آنها از یک آستانه‌ای بیشتر باشد، به عنوان خوشه‌های مشکوک نشانه‌گذاری شده و میزبان‌های موجود در این خوشه‌ها به ماتریس فعالیت‌های گروهی مشکوک اضافه می‌شوند. در ادامه، نحوه انجام این فرایند به طور کامل توضیح داده می‌شود.

قبل از خوشه‌بندی نام‌های دامنه، ویژگی‌های ذکرشده نرمال‌سازی می‌شوند و مقدار هر ویژگی بین ۰ و ۱ نرمال می‌شود. نرمال‌کردن این ویژگی‌ها به این دلیل است که اختلاف‌های زیاد بین مقادیر ویژگی‌های متفاوت، تأثیر کمتری بر روی فرایند خوشه‌بندی داشته باشد. در روش پیشنهادی، به منظور نرمال‌سازی ویژگی‌ها در هر پنجره زمانی از روش مقیاس‌گذاری خطی[3] استفاده شده است [۱۴]

$$x_i^* = \frac{x_i - x_{\min}}{x_{\max} - x_{\min}} \quad , \quad i = 1,2,\ldots,10 \qquad (۴)$$

که در آن x_i^* مقدار نرمال‌شده ویژگی iام، $x_{\min}$ حداقل مقدار ویژگی iام و $x_{\max}$ حداکثر مقدار ویژگی iام است.

تعریف ۱۰ (خوشه): هر خوشه شامل مجموعه‌ای از پرس و جوهای DNS است که فاصله اقلیدسی[4] بردار ویژگی این پرس و جوها تا مرکز خوشه از شعاع ثابت ω کمتر است. هر خوشه c_j دارای یک مرکز است که با $\mu(c_j)$ نمایش داده می‌شود. $\mu(c_j)$ یک بردار ویژگی هفت‌بُعدی است. مقدار مرکز خوشه از میانگین مقادیر بردارهای ویژگی پرس و جوهای DNS عضو خوشه c_j حاصل شده و مجموعه خوشه‌ها در هر دوره زمانی t با $C(t)$ نمایش داده می‌شود.

تعریف ۱۱ (فاصله اقلیدسی): در ریاضیات، فاصله اقلیدسی فاصله بین دو نقطه است که توسط قضیه فیثاغورس به دست می‌آید [۱۵]. اگر $p = (p_1, p_2, \ldots, p_n)$ و $q = (q_1, q_2, \ldots, q_n)$ دو نقطه در فضای n بعدی باشند، آن گاه فاصله اقلیدسی بین آنها از (۵) محاسبه می‌شود

$$d(P,Q) = \sqrt{(p_1 - q_1)^2 + (p_2 - q_2)^2 + \ldots + (p_n - q_n)^2} \qquad (۵)$$

شبه‌کد الگوریتم خوشه‌بندی با شعاع ثابت در شکل ۱ نشان داده شده است. این الگوریتم بردارهای ویژگی پرس و جوهای DNS در پنجره زمانی فعلی و شعاع ثابت ω را به عنوان ورودی دریافت کرده و در

1. Shannon Entropy

2. Autonomous System

3. Linear Scaling to Unit Range

4. Euclidean Distance

Algorithm *FWC*

input:
$D(t)$: set of DNS query feature vectors
ω : fixed radius
output:
$C(t)$: set of clusters

1. $C(t) \leftarrow \phi$
2. **for** each $d_i \in D(t)$ **do**
3. **if** $C(t) = \phi$ **then**
4. $c_{new} \leftarrow \{d_i\}$
5. $\mu(c_{new}) \leftarrow d_i$
6. $C(t) \leftarrow \{c_{new}\}$
7. **else**
8. $c_{\min} \leftarrow \arg\min_{c_j \in C(t)} \theta_d(d_i, \mu(c_j))$
9. **if** $\theta_d(d_i, \mu(c_{\min})) < \omega$ **then**
10. $c_{\min} \leftarrow c_{\min} \cup \{d_i\}$
11. $\mu(c_{\min}) \leftarrow \frac{1}{|c_{\min}|} \sum_{d_j \in c_{\min}} d_j$
12. **else**
13. $c_{new} \leftarrow \{d_i\}$
14. $\mu(c_{new}) \leftarrow d_i$
15. $C(t) \leftarrow C(t) \cup \{c_{new}\}$
16. **end if**
17. **end if**
18. **end for**
19. **return** $C(t)$

شکل ۱: شبه‌کد الگوریتم خوشه‌بندی با شعاع ثابت.

خروجی مجموعه $C(t)$ را به عنوان مجموعه خوشه‌های ایجادشده تحویل می‌دهد.

در خط اول، مقدار تهی به مجموعه $C(t)$ نسبت داده شده و سپس مراحل زیر برای تمام پرس و جوهای DNS موجود در $D(t)$ تکرار می‌شوند (خطوط ۲ تا ۱۸). اگر مجموعه $C(t)$ برابر تهی باشد، خوشه جدید c_{new} با مرکز d_i ایجاد و به مجموعه $C(t)$ اضافه می‌شود (خطوط ۳ تا ۶). در غیر این صورت d_i به نزدیک‌ترین خوشه $c_{\min}$ موجود در $C(t)$ که فاصله اقلیدسی بین بردار ویژگی d_i و $\mu(c_{\min})$ از آستانه ω کمتر بوده اضافه شده و مرکز خوشه $c_{\min}$ با استفاده از میانگین بردارهای ویژگی پرس و جوهای DNS موجود در $c_{\min}$ به روز رسانی می‌شود (خطوط ۷ تا ۱۱). در خط ۸ از شبه‌کد، نزدیک‌ترین خوشه به بردار ویژگی پرس و جوی d_i شناسایی شده و در صورتی که فاصله اقلیدسی این بردار از خوشه مشخص‌شده کمتر از شعاع ثابت ω باشد (خط ۹) پرس و جوی d_i به خوشه تعیین‌شده اضافه می‌شود (خط ۱۰) و سپس مرکز خوشه با استفاده از میانگین فاصله اقلیدسی بین تمام بردارهای ویژگی پرس و جوهای DNS موجود در آن خوشه با مرکز خوشه به روز رسانی می‌شود (خط ۱۱). اگر فاصله اقلیدسی بین بردار ویژگی d_i و $\mu(c_{\min})$ از آستانه ω کمتر نباشد، خوشه جدید c_{new} با مرکز d_i ایجاد شده و این خوشه جدید به مجموعه خوشه‌های قبلی اضافه می‌شود (خطوط ۱۲ تا ۱۵).

۳-۲-۳ شناسایی فعالیت‌های گروهی مشکوک

در روش پیشنهادی پس از انجام عمل خوشه‌بندی نام‌های دامنه، نیاز به روالی داریم تا فعالیت‌های گروهی مشکوک میزبان‌ها در خوشه‌های مختلف را شناسایی کند. برای رسیدن به این هدف، ایده پیشنهادی چنین تعریف می‌شود که از یک معیار شباهت بین خوشه‌ها استفاده کنیم.

Algorithm *SGAD*

input:
$D(t)$: set of DNS query feature vectors
ω : fixed radius
τ_s : similarity threshold
output:
$\delta(t)$: set of suspicious group activities

1. $C(t) \leftarrow FWC(D(t), \omega)$
2. $\delta(t) \leftarrow \phi$
3. **for** each cluster $c_j \in C(t)$ **do**
4. Calculate the similarity criterion $\theta_s(c_j)$
5. **if** $|c_j| \geq 2$ **and** $\theta_s(c_j) > \tau_s$ **then**
6. $\delta(t) \leftarrow \delta(t) \cup c_j$
7. **end if**
8. **end for**
9. **return** $\delta(t)$

شکل ۲: شبه‌کد الگوریتم شناسایی فعالیت‌های گروهی مشکوک.

تعریف ۱۲ (شباهت بین خوشه‌ها): معیار شباهت درون‌خوشه‌ای در خوشه c_j با $\theta_s(c_j)$ نشان داده شده و با استفاده از (۶) محاسبه می‌شود

$$\theta_s(c_j) = e^{-\bar{d}_j} \qquad (۶)$$

که $\bar{d}_j$ متوسط فاصله بردارهای ویژگی تمام پرس و جوهای DNS عضو خوشه c_j تا مرکز این خوشه است و متوسط فاصله درون‌خوشه‌ای نامیده می‌شود

$$\bar{d}_j = \frac{1}{|c_j|} \sum_{d_i \in c_j} \theta_d(d_i, \mu(c_j)) \qquad (۷)$$

θ_d فاصله اقلیدسی بین دو بردار ویژگی است. همان طور که در (۶) مشخص است هرچه متوسط فاصله درون‌خوشه‌ای کمتر باشد، شباهت درون‌خوشه‌ای افزایش می‌یابد.

شبه‌کد الگوریتم شناسایی فعالیت‌های گروهی مشکوک (SGAD) در شکل ۲ نشان داده شده است. این الگوریتم بردارهای ویژگی پرس و جوهای DNS در پنجره زمانی فعلی، شعاع ثابت ω و آستانه شباهت τ_s را به عنوان ورودی دریافت کرده و در خروجی مجموعه $\delta(t)$ را به عنوان فعالیت‌های گروهی مشکوک تحویل می‌دهد.

در ابتدا الگوریتم خوشه‌بندی با شعاع ثابت بر روی مجموعه $D(t)$ فراخوانی شده تا مجموعه خوشه‌های $C(t)$ ایجاد شوند (خط ۱). سپس برای شروع عملیات، مجموعه $\delta(t)$ که به عنوان فعالیت‌های گروهی مشکوک می‌باشد با تهی مقداردهی می‌شود (خط ۲). بعد از این مرحله، میزان شباهت درون‌خوشه‌ای به ازای تمام خوشه‌های c_j موجود در $C(t)$ محاسبه می‌شود (خط ۴). اگر خوشه c_j شامل حداقل دو پرس و جوی DNS متفاوت بوده و میزان شباهت درون‌خوشه‌ای آن از آستانه شباهت τ_s بیشتر باشد (خط ۵)، آن گاه تمام پرس و جوهای DNS موجود در خوشه c_j به $\delta(t)$ اضافه می‌شوند (خط ۶). همان طور که اشاره شد، این الگوریتم بر روی تمامی خوشه‌های ایجادشده عمل کرده و خروجی حاصل که شامل فعالیت‌های گروهی مشکوک می‌باشد در مجموعه $\delta(t)$ تحویل داده می‌شود.

پس از انجام مراحل فوق، میزبان‌هایی که دارای حداقل یک پرس و جوی DNS در مجموعه $\delta(t)$ باشند به ماتریس فعالیت‌های گروهی مشکوک اضافه می‌شوند تا میزان شهرت منفی آنها محاسبه شود.

جدول ۲: مشخصات ترافیک‌های استفاده‌شده در آزمایش‌ها.

مشخصات ترافیک	Conficker	Cycbot	Zeus	Storm	Rock	Murofet	ترافیک عادی
تعداد پرس و جوهای DNS	۱۴۲۱۸	۴۳۲۵	۹۸۲	۷۴۲۸	۴۲۷۳	۹۸۱۷	$۲۸/۳۹۵\times۱۰^{۵}$
زمان آزمایش	۷ ساعت	۷ ساعت	۷ ساعت	۷ ساعت	۷ ساعت	۷ ساعت	۷ ساعت
تعداد میزبان‌ها	۱۰	۱۰	۱۰	۱۰	۱۰	۱۰	۲۱۴۵

۳-۲-٤ محاسبه شهرت منفی میزبان‌ها

هدف مهم روش پیشنهادی، برقراری توازن بین داشتن حداقل نرخ هشدار نادرست و عدم تغییر در نرخ تشخیص میزبان‌های آلوده است. ایده به کار گرفته شده برای رسیدن به این هدف این است که در پایان هر پنجره زمانی شهرت منفی برای میزبان‌هایی محاسبه شود که در این پنجره زمانی به ماتریس فعالیت‌های گروهی مشکوک اضافه شده‌اند و میزبان‌های دارای شهرت منفی بالا به عنوان میزبان‌های آلوده به بات گزارش می‌شوند.

هنگام محاسبه میزان شهرت یک میزبان، قابلیت اطمینان آن شهرت از اهمیت زیادی برخوردار است. هر چند این قابلیت اطمینان تابع عوامل متعددی است، در این مقاله محاسبه شهرت منفی مبتنی بر فعالیت‌های گروهی مشکوک و سابقه این فعالیت‌ها در m پنجره زمانی قبلی انجام می‌شود.

الف) سابقه فعالیت‌های مشکوک در پنجره‌های زمانی متفاوت

در یک شبکه تحت نظارت، مشاهدات کم از فعالیت‌های مشکوک یک میزبان برای داوری در مورد شهرت منفی آن میزبان کافی نیست. بنابراین در روش پیشنهادی به میزبان‌هایی که سابقه بیشتری از فعالیت‌های مشکوک داشته باشند شهرت منفی بیشتری نسبت داده می‌شود. با فرض این که t پنجره زمانی جاری و G ماتریس فعالیت‌های گروهی مشکوک باشد، برای هر میزبان h_i سابقه فعالیت گروهی مشکوک در m پنجره زمانی قبلی با $\iota_g(h_i,G,t)$ نمایش داده می‌شود

$$\iota_g(h_i,G,t)=\begin{cases}\sin(\frac{\pi}{۲}\cdot\beta(h_i,G,t)) & ,\ \beta(h_i,G,t)\in[۰,\varepsilon)\\ ۱ & ,\ \text{otherwise}\end{cases} \quad (۸)$$

که $\varepsilon<m$ پارامتری است که توسط کاربر تعیین شده و میزان اهمیت سابقه فعالیت‌های گروهی مشکوک را نشان می‌دهد. $\beta(h_i,G,t)$ تعداد پنجره‌های زمانی است که میزبان h_i در آنها فعالیت گروهی مشکوک داشته است

$$\beta(h_i,G,t)=\sum_{\tau=t}^{t-m+۱} g_{i\tau} \quad (۹)$$

ب) شباهت شرکت‌کننده‌ها در فعالیت‌های گروهی مشکوک

از آنجایی که میزبان‌های آلوده به بات، کد مخرب یکسانی را اجرا می‌کنند، بنابراین انتظار می‌رود که در پنجره‌های زمانی متفاوت، میزبان‌های مشارکت‌کننده در فعالیت‌های مشکوک تنوع کمی داشته باشند. به عبارت دیگر اگر در پنجره‌های زمانی متفاوت، میزبان‌های مختلفی در فعالیت‌های مشکوک مشارکت داشته باشند، احتمال کمی وجود دارد که این میزبان‌ها به بات آلوده شده باشند. بنابراین در روش پیشنهادی در هر پنجره زمانی برای هر میزبان مشارکت‌کننده در یک فعالیت مشکوک، فهرستی از سایر میزبان‌های مشارکت‌کننده در این فعالیت نگهداری می‌شود. هرچه تنوع میزبان‌های این فهرست در پنجره‌های زمانی متفاوت کمتر باشد شهرت منفی بیشتری به آن میزبان نسبت داده می‌شود.

با فرض این که h_i میزبانی باشد که در پنجره زمانی جاری t در یک فعالیت مشکوک مشارکت داشته است و $\delta(h_i,G,t)$ فهرست سایر میزبان‌های مشارکت‌کننده با h_i در این فعالیت مشکوک باشند، شباهت میزبان‌های این فهرست در پنجره‌های زمانی متفاوت با استفاده از معیار شباهت جاکارد [۱۶] و (۱۰) محاسبه می‌شود

$$\gamma_s(h_i,G,t)=\frac{۱}{m-۱}\sum_{\tau=t-۱}^{t-m+۱}\frac{|\delta(h_i,G,t)\cap\delta(h_i,G,\tau)|}{|\delta(h_i,G,t)\cup\delta(h_i,G,\tau)|} \quad (۱۰)$$

ج) به روز رسانی شهرت منفی

شهرت منفی هر میزبان h_i در پایان پنجره زمانی t با $R(h_i,G,t)$ نمایش داده شده و با استفاده از رابطه زیر محاسبه می‌شود

$$R(h_i,G,t)=w_۱\cdot\iota_g(h_i,G,t)+w_۲\cdot\gamma_s(h_i,G,t) \quad (۱۱)$$

که در آن $w_۱=w_۲=۰/۵$ است. در صورتی که شهرت منفی میزبان h_i از یک آستانه ξ بیشتر شود، این میزبان به عنوان یک میزبان آلوده به بات گزارش می‌شود.

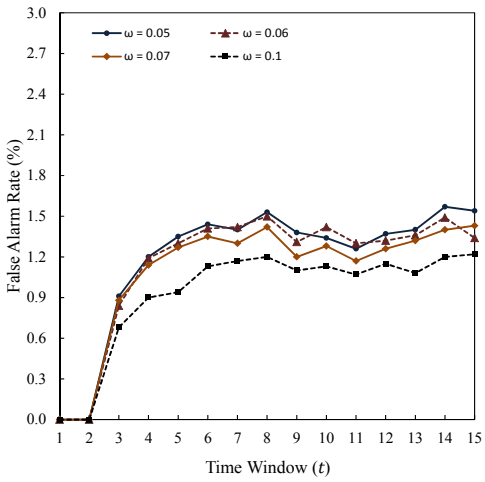
٤- ارزیابی روش پیشنهادی

در این بخش، روش پیشنهادی برای تشخیص بات‌نت‌ها مورد ارزیابی قرار می‌گیرد. ابتدا نحوه جمع‌آوری ترافیک شبکه استفاده‌شده در آزمایش‌ها تشریح شده و سپس نتایج ارزیابی‌های مختلف انجام‌شده به همراه تحلیل آنها ارائه می‌شود. در این ارزیابی‌ها تأثیر پارامترهای مختلف بر روی روش پیشنهادی نشان داده شده و تحلیلی از میزان حساسیت این روش نسبت به مقادیر مختلف پارامترها ارائه می‌شود. از طریق این تحلیل‌ها، می‌توان مقادیر مناسب این پارامترها را برای تشخیص بهتر میزبان‌های آلوده به بات تخمین زد. در ادامه در بخش ۴-۳ مقایسه بین روش پیشنهادی و سایر روش‌ها ارائه می‌شود.

٤-۱ جمع‌آوری ترافیک شبکه

برای تولید ترافیک واقعی بات‌ها، یک بستر آزمایشگاهی شامل ده میزبان مجازی VMware پیاده‌سازی شد. در آزمایش‌های مختلف، این میزبان‌ها به بات‌های Conficker، Cycbot، Zeus، Storm، Rock و Murofet [۱۷] آلوده شدند. از ترافیک DNS میزبان‌های آلوده به بات برای محاسبه نرخ تشخیص و از ترافیک DNS سایر میزبان‌ها در شبکه دانشگاه (به عنوان ترافیک عادی) برای محاسبه نرخ هشدار نادرست روش پیشنهادی استفاده شد. ترافیک DNS میزبان‌های آلوده به بات و ترافیک DNS دانشگاه در آزمایش‌های مختلف و با استفاده از ابزار TCP Replay دوباره ارسال شده و نتیجه حاصل از ادغام آنها به عنوان ترافیک ورودی در آزمایش‌ها به کار گرفته شد.

مشخصات ترافیک‌های فوق در جدول ۲ نمایش داده شده است. قابل ذکر است که محدوده آدرس‌های IP متعلق به شبکه‌های خودمختار متفاوت از [۱۸] به دست آمده است.



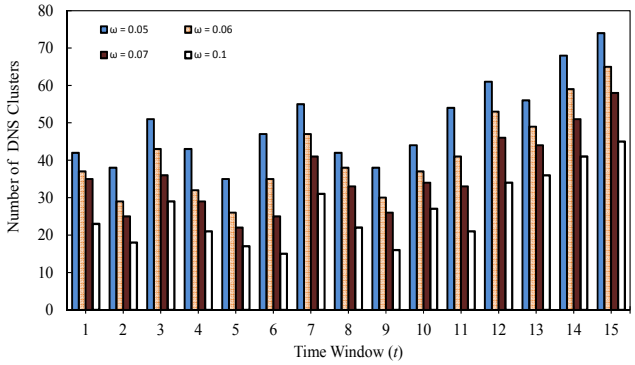
شکل ۳: نرخ هشدار نادرست سیستم پیشنهادی به ازای مقادیر مختلف ω.

۴-۲ نتایج ارزیابی

بات‌نت‌های مختلف از روش‌های متفاوتی برای به دست آوردن آدرس سرویس‌دهنده فرمان و کنترل خود استفاده می‌کنند. در نتیجه برای تعیین مقدار شعاع ثابت ω به منظور خوشه‌بندی، مقدار آستانه شباهت درون‌خوشه‌ای τ_s و مقدار آستانه تشخیص آلودگی ξ، از میان یک میلیون وب‌سایت برتر گزارش‌شده توسط Alexa [۱۰] هزار نام دامنه به صورت تصادفی انتخاب شده و توزیع دوتایی‌ها برای آنها محاسبه شد. همچنین ترافیک DNS ایجادشده توسط دو بات‌نت Conficker و Rock نیز ضبط شد و نام‌های دامنه ضبط‌شده با نام‌های دامنه هزار وب‌سایت برتر مرحله قبل ترکیب شد. از ترافیک به دست آمده به عنوان ورودی روش پیشنهادی استفاده و این روش ۲۰ مرتبه تکرار شد. بر مبنای نتایج این تکرارها، آستانه‌های ω، τ_s و ξ به ترتیب به ۰٫۰۵، ۰٫۸ و ۰٫۶ مقداردهی شدند. همچنین اندازه پنجره‌های زمانی برابر ۲۰ دقیقه در نظر گرفته شده است. به پارامتر m که نشان‌دهنده تعداد پنجره‌های زمانی برای محاسبه شهرت منفی است، مقدار ۵ نسبت داده شد. در محاسبه شهرت منفی هرچه سابقه بیشتری از فعالیت‌های مشکوک میزبان‌ها در نظر گرفته شود، میزان هشدار نادرست روش پیشنهادی کمتر می‌شود. بنابراین به پارامتر ε که نشان‌دهنده اهمیت سابقه فعالیت‌های گروهی مشکوک است مقدار ۳ نسبت داده شد.

در شکل ۳ نرخ هشدار نادرست سیستم پیشنهادی در پنجره‌های زمانی متوالی و به ازای مقادیر مختلف شعاع خوشه‌بندی ω آمده است. همان طور که مشاهده می‌شود با نسبت‌دادن مقادیر بیشتر به شعاع خوشه‌بندی ω، نرخ هشدار نادرست کاهش می‌یابد. در این حالت، دلیل کاهش نرخ هشدار نادرست این است که با افزایش ω، بردارهای ویژگی پرس و جوهای DNS موجود در هر خوشه فاصله بیشتری نسبت به مرکز آن خوشه پیدا کرده و در نتیجه باعث کاهش شباهت درون‌خوشه‌ای می‌شوند. این مسأله منجر می‌شود تا شباهت درون‌خوشه‌ای خوشه‌های غیر بات‌نت کمتر شده و نرخ هشدار نادرست کاهش یابد.

در شکل ۴ تأثیر مقادیر مختلف شعاع خوشه‌بندی ω بر روی تعداد خوشه‌های ایجادشده در روش پیشنهادی نشان داده شده است. نتایج نشان داده شده در این شکل با استفاده از پرس و جوهای DNS بات‌نت Cycbot و ترافیک DNS میزبان‌های دانشگاه به دست آمده است. همان طور که در این شکل مشاهده می‌شود، با افزایش ω تعداد خوشه‌های ایجادشده در هر دوره زمانی کاهش می‌یابد.



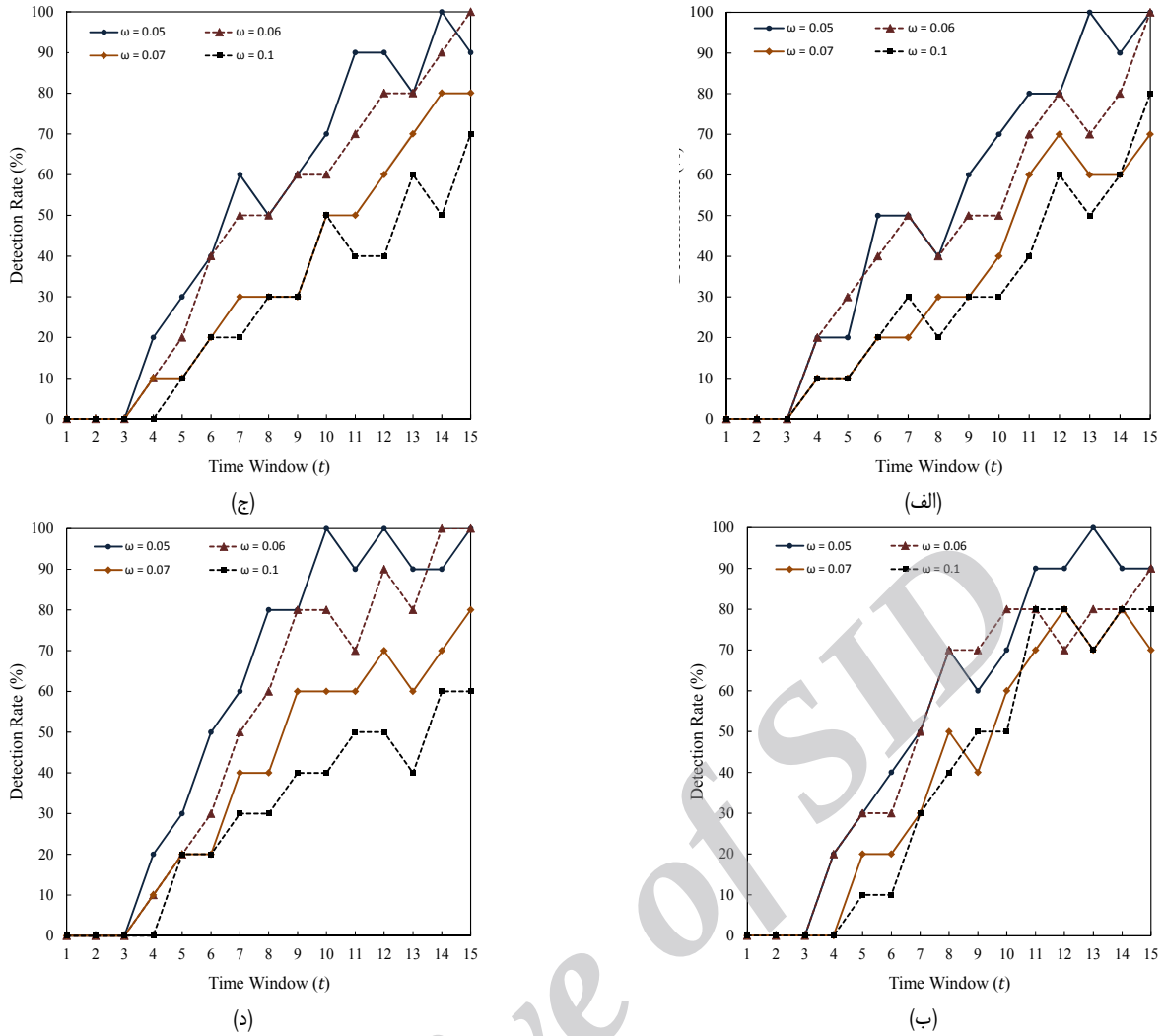
شکل ۴: تأثیر مقادیر مختلف شعاع خوشه‌بندی ω بر روی تعداد خوشه‌ها.

در شکل ۵ نرخ تشخیص سیستم پیشنهادی در پنجره‌های زمانی متوالی و به ازای مقادیر مختلف شعاع خوشه‌بندی ω نشان داده شده است. همان طور که در این شکل مشاهده می‌شود مقادیر بیشتر شعاع خوشه‌بندی ω باعث کاهش نرخ تشخیص می‌شود. همان طور که پیش از این گفته شد در سیستم پیشنهادی سعی بر شناسایی خوشه‌هایی است که دارای بردارهای ویژگی مرتبط با فعالیت‌های هماهنگ گروهی مشکوک هستند. بنابراین با افزایش ω بردارهای ویژگی پرس و جوهای DNS غیر بات‌نت به خوشه‌های بات‌نت اضافه شده و شباهت درون‌خوشه‌ای آن را کاهش می‌دهند. در نتیجه، این مسأله منجر می‌شود تا آنها به عنوان خوشه‌های مشکوک در نظر گرفته نشده و نرخ تشخیص کاهش یابد. همچنین نرخ تشخیص بات‌نت‌های مختلف به تدریج اضافه شده تا به مقدار ۱۰۰٪ برسد و این اضافه‌شدن تدریجی به این دلیل است که به مرور زمان و با انجام فعالیت‌های مشکوک توسط میزبان‌های آلوده، میزان شهرت منفی آنها اضافه می‌شود. با این وجود در صورتی که تعدادی از میزبان‌های آلوده در چندین پنجره زمانی متوالی فعالیت‌های مشکوک نداشته باشند از میزان شهرت منفی آنها کاسته می‌شود.

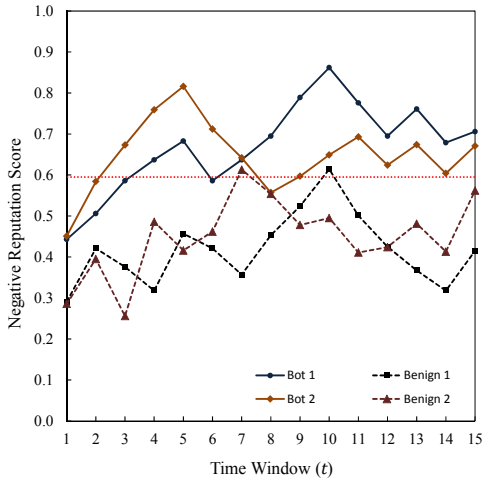
همان طور که بیان شد، میزبان‌های آلوده به بات در فعالیت‌های هماهنگ گروهی مشکوکی مشارکت می‌کنند. بنابراین پس از شناسایی خوشه‌های مشکوک و اضافه‌کردن میزبان‌های شرکت‌کننده در این خوشه‌ها به ماتریس فعالیت‌های گروهی مشکوک، محاسبه‌کننده شهرت منفی میزبان‌ها یک امتیاز شهرت منفی برای هر میزبان مشکوک محاسبه می‌کند. شکل ۶ امتیاز شهرت منفی میزبان‌های غیر آلوده Benign ۱ و Benign ۲ و میزبان‌های آلوده Bot ۱ و Bot ۲ را نشان می‌دهد. میزبان‌های غیر آلوده Benign ۱ و Benign ۲ به طور تصادفی از بین تمامی میزبان‌هایی انتخاب شده‌اند که حداقل در یک پنجره زمانی امتیاز شهرت منفی آنها بالاتر از آستانه تشخیص آلودگی ξ بوده است. همچنین میزبان‌های آلوده Bot ۱ و Bot ۲ به طور تصادفی از بین ده میزبان آلوده به بات‌نت Cycbot انتخاب شده‌اند.

به دلیل این که Benign ۱ و Benign ۲ در یک فعالیت هماهنگ گروهی مشکوک به همراه چندین میزبان غیر آلوده دیگر شرکت کرده‌اند، یک امتیاز شهرت منفی به دست آورده‌اند. در سوی دیگر، Bot ۱ و Bot ۲ در فعالیت‌های هماهنگ گروهی در چندین دوره زمانی مشارکت داشته‌اند. در نتیجه امتیاز شهرت منفی آنها به طور تدریجی افزایش پیدا کرده است. این مسأله نشان می‌دهد که این میزبان‌ها آلوده به بات هستند (مقدار آستانه تشخیص آلودگی ξ در شکل ۶ با خط‌چین قرمز نشان داده شده است).

به منظور نشان‌دادن تأثیر استفاده از سابقه فعالیت‌های مشکوک در نرخ تشخیص و نرخ هشدار نادرست روش پیشنهادی، آزمایش جداگانه‌ای به



شکل ۵: نرخ تشخیص سیستم پیشنهادی بر اساس مقادیر مختلف ω، (الف) Cycbot، (ب) Zeus، (ج) Murofet و (د) Storm.



شکل ۶: امتیاز شهرت منفی میزبان‌های غیر آلوده و آلوده به بات‌نت Cycbot.

ازای مقادیر مختلف پارامتر m و $\varepsilon = ۰/۶m$ انجام شد. جهت انجام این آزمایش‌ها از بات‌نت Cycbot استفاده شده است. جدول ۳ نتایج حاصل از این آزمایش را نشان می‌دهد. همان گونه که مشاهده می‌شود روش پیشنهادی به ازای $m = ۱$ در پنجره‌های زمانی مختلف دارای نرخ هشدار نادرست بالایی است به دلیل این که در این حالت سابقه فعالیت‌های گروهی مشکوک میزبان‌ها بررسی نمی‌شود. در نتیجه، قبل از به دست آمدن اطلاعات کافی در مورد آلودگی میزبان‌ها، پیش‌داوری اشتباهی از آنها انجام گرفته و گزارش می‌شود. همچنین به ازای $m = ۵$، روش پیشنهادی به ترتیب نرخ هشدار نادرست کمتر و بیشتری نسبت به حالت‌های $m = ۱$ و $m = ۱۰$ دارد که دلیل این امر این است که به ازای مقادیر بیشتر پارامترهای m و ε، روش پیشنهادی به سابقه فعالیت‌های گروهی مشکوک میزبان‌ها اهمیت بیشتری می‌دهد، در حالی که تأثیر کمی روی نرخ تشخیص دارد.

۴-۳ مقایسه‌ها

به دلیل وجود تفاوت بین شبکه‌های مورد ارزیابی و استفاده از بات‌های متفاوت در آزمایش‌ها، نمی‌توان مقایسه کاملی بین روش‌های مختلف انجام داد. بنابراین روش پیشنهادی و سایر روش‌ها با توجه به چندین معیار با یکدیگر مقایسه می‌شوند که قابلیت‌های روش‌ها را نشان می‌دهند. در ادامه این بخش، ابتدا معیارهای مقایسه معرفی شده و سپس مقایسه‌ای بین روش پیشنهادی و سایر روش‌های بیان‌شده انجام می‌شود.

تشخیص مبتنی بر فعالیت گروهی در ترافیک DNS: این معیار مشخص می‌کند که آیا روش مذکور در شناسایی بات‌نت‌ها به بررسی فعالیت گروهی میزبان‌های آلوده که یک ویژگی ذاتی در هر بات‌نتی است توجه دارد یا خیر.

تشخیص مبتنی بر سابقه فعالیت‌های مشکوک: بر اساس این معیار تصمیم‌گیری در مورد آلوده‌بودن یک میزبان با مشاهده فعالیت‌های مشکوک توسط آن میزبان در چندین دوره زمانی متوالی انجام می‌پذیرد.

جدول ۳: نرخ تشخیص و هشدار نادرست روش پیشنهادی.

پنجره زمانی	$m=۱$		$m=۵$		$m=۱۰$	
	نرخ تشخیص	نرخ هشدار نادرست	نرخ تشخیص	نرخ هشدار نادرست	نرخ تشخیص	نرخ هشدار نادرست
۱	۱۰	۰٫۵۱	۰	۰	۰	۰
۲	۲۰	۱٫۰۱	۱۰	۰٫۳۸	۰	۰٫۱۵
۳	۴۰	۱٫۱۶	۲۰	۰٫۶۱	۱۰	۰٫۲۱
۴	۷۰	۱٫۸۷	۴۰	۰٫۹۱	۳۰	۰٫۲۸
۵	۸۰	۲٫۲۶	۶۰	۱٫۰۸	۶۰	۰٫۴۷
۶	۹۰	۲٫۴۷	۷۰	۱٫۲۳	۶۰	۰٫۷۲
۷	۱۰۰	۲٫۸۳	۹۰	۱٫۶۱	۸۰	۰٫۸۱
۸	۱۰۰	۲٫۹	۸۰	۱٫۸۰	۷۰	۰٫۷۱
۹	۹۰	۲٫۷۳	۹۰	۱٫۹۲	۷۰	۰٫۹۲
۱۰	۹۰	۲٫۵۸	۹۰	۱٫۶۱	۸۰	۱٫۰۶
۱۱	۱۰۰	۲٫۲۲	۱۰۰	۱٫۷۱	۱۰۰	۱٫۱۴
۱۲	۱۰۰	۲٫۵۴	۱۰۰	۱٫۵۷	۱۰۰	۱٫۰۳
۱۳	۸۰	۲٫۸۱	۸۰	۱٫۹۵	۸۰	۱٫۲۴
۱۴	۱۰۰	۳٫۰۷	۱۰۰	۲٫۰۳	۹۰	۱٫۳۱
۱۵	۹۰	۳٫۲۷	۹۰	۱٫۷۶	۸۰	۱٫۰۹

جدول ۴: مقایسه روش پیشنهادی با سایر روش‌های تشخیص بات‌نت مبتنی بر ترافیک DNS.

روش تشخیص بات‌نت‌ها	تشخیص مبتنی بر فعالیت گروهی در ترافیک DNS	تشخیص مبتنی بر سابقه فعالیت‌های مشکوک	تشخیص تغییر پی‌درپی نام دامنه	تشخیص تغییر پی‌درپی آدرس IP	تشخیص زیردامنه‌های تصادفی
[۲] Holz	×	×	×	✓	✓
[۳] Yadav	✓	×	✓	×	✓
[۴] Yadav	×	×	✓	×	×
[۵] Kruegel	✓	×	✓	✓	✓
[۶] Antonakakis	✓	×	✓	×	×
[۷] Choi	✓	×	✓	×	✓
[۸] Davuth	✓	×	✓	×	✓
سیستم پیشنهادی	✓	✓	✓	✓	✓

تشخیص تغییر پی‌درپی نام دامنه: نشان می‌دهد که آیا روش مورد بررسی قادر به شناسایی بات‌نت‌های مبتنی بر تغییر پی‌درپی نام دامنه است یا خیر.

تشخیص تغییر پی‌درپی آدرس IP: نشان می‌دهد که روش مورد بررسی قادر به شناسایی بات‌نت‌های مبتنی بر تغییر پی‌درپی آدرس IP است یا خیر.

تشخیص زیردامنه‌های تصادفی: به منظور نشان‌دادن عدم کارایی روش‌هایی به کار می‌رود که به منظور شناسایی بات‌نت‌ها، تنها از درخواست‌های ناموفق DNS استفاده می‌کنند. این روش‌ها به سادگی در مقابل استفاده از چنین تکنیک‌هایی توسط مدیران بات در تشخیص بات‌نت‌ها با شکست مواجه می‌شوند.

در جدول ۴ روش پیشنهادی با سایر روش‌های تشخیص بات‌نت مبتنی بر ترافیک DNS مقایسه شده است. به دلیل این که روش پیشنهادی از یک تکنیک غیر نظارتی برگرفته از ویژگی‌های ذاتی بات‌نت‌ها (انجام فعالیت‌های یکسان و فعالیت‌های گروهی هماهنگ) استفاده می‌کند، قادر است تا بات‌نت‌های شناخته‌شده و ناشناخته را تشخیص دهد بدون آن که دانش قبلی از آنها داشته باشد.

۵- نتیجه‌گیری

امروزه بات‌نت‌ها به عنوان مهم‌ترین تهدید اینترنتی شناخته شده‌اند که به‌طور پیوسته در حال رشد و گسترش می‌باشند. یک بات‌نت، شبکه‌ای از میزبان‌هایی است که به کد بدخواه یکسانی آلوده شده و این اجازه را به مهاجم (مدیر بات) می‌دهند تا آنها را با استفاده از یک یا چند سرویس‌دهنده فرمان و کنترل و از راه دور هدایت نماید.

در این مقاله، یک روش خوشه‌بندی به همراه محاسبه شهرت منفی هر میزبان برای تشخیص برخط بات‌نت‌ها با استفاده از ترافیک DNS پیشنهاد شد که از رفتار هماهنگ و گروهی بات‌ها (میزبان‌های آلوده) در فرایند تشخیص استفاده می‌کند. سیستم پیشنهادی بر این واقعیت استوار است که بات‌های عضو یک بات‌نت یکسان، کد دودویی یکسانی را اجرا می‌کنند که توسط مدیر بات نوشته شده است. بنابراین آنها الگوی ارتباطی و فعالیت‌های مشکوک مشابهی را از خود نشان می‌دهند. این مسأله منجر به انجام فعالیت‌های گروهی هماهنگ در مراحل مختلفی از چرخه حیات بات‌نت می‌شود که از آن برای شناسایی میزبان‌های آلوده به بات استفاده شده است. با توجه به این رفتار هماهنگ گروهی بین بات‌ها، ایده محاسبه شهرت منفی برای میزبان‌های مختلف در پنجره‌های زمانی پشت سر هم ارائه شد تا نرخ هشدار نادرست کاهش پیدا کند. روش پیشنهادی با

استفاده از دو معیار نرخ تشخیص و نرخ هشدار نادرست مورد ارزیابی قرار گرفت. برای محاسبه این دو معیار به ترتیب از ترافیک DNS میزبان‌های آلوده به بات و ترافیک DNS میزبان‌های غیر آلوده در شبکه دانشگاه استفاده شد. نتایج آزمایش‌ها نشان می‌دهند که روش پیشنهادی قادر است بات‌نت‌هایی که از تکنیک‌های گریز مبتنی بر سرویس DNS برای پنهان‌ماندن سرویس‌دهنده‌های فرمان و کنترل خود استفاده می‌کنند را با توجه به سابقه فعالیت‌های گروهی مشکوک و مستقل از ساختار و پروتکل فرمان و کنترل آنها با نرخ تشخیص بالا و نرخ هشدار نادرست پایین شناسایی کند.

مراجع

[1] S. S. C. Silva, R. M. P. Silva, R. C. G. Pinto, and R. M. Salles, "Botnets: a survey," *Computer Networks: the International J. of Computer and Telecommunications Networking*, vol. 57, no. 2, pp. 378-403, Feb. 2013.

[2] T. Holz, C. Gorecki, K. Rieck, and F. C. Freiling, "Measuring and detecting fast-flux service networks," in *Proc. 15th Network and Distributed System Security Symp., NDSS'08*, 12 pp., San Diego, California, USA, Feb. 2008.

[3] S. Yadav, A. K. Krishna Reddy, A. L. Reddy, and S. Ranjan, "Detecting algorithmically generated malicious domain names," in *Proc. of the 10th ACM SIGCOMM Conf. on Internet Measurement, ACM*, pp. 48-61, New York, NY, USA, 1-3 Nov. 2010.

[4] S. Yadav and A. L. Narasimha Reddy, "Winning with DNS failures: strategies for faster botnet detection," in *Proc. of the 7th International ICST Conf. on Security and Privacy in Communication Networks, SecureComm'11*, vol. 96, pp. 446-459, London, UK, 2011.

[5] C. Kruegel, L. Bilge, E. Kirda, and M. Balduzzi, "Exposure: finding malicious domains using passive DNS analysis," in *Proc. of 18th Network and Distributed System Security Symp., NDSS'11*, pp. 214-231, San Diego, California, USA, 6-9 Feb. 2011.

[6] M. Antonakakis, *et al*., "From throw-away traffic to bots: detecting the rise of DGA-based malware," in *Proc. of 21th USENIX Security Symp.,* pp. 24-40, Bellevue, WA, USA, Aug. 2012.

[7] H. Choi and H. Lee, "Identifying botnets by capturing group activities in DNS traffic," *Computer Networks: the International J. of Computer and Telecommunications Networking*, vol. 56, no. 1, pp. 20-33, Jan. 2012.

[8] N. Davuth and S. R. Kim, "Classification of malicious domain names using support vector machine and bi-gram method," *International J. of Security and Its Applications, IJSIA*, vol. 7, no. 1, pp. 51-58, Jan. 2013.

[9] S. Jordi and C. Sierra, "REGRET: reputation in gregarious societies," in *Proc. of the 5th ACM International Conf. on Autonomous Agents*, pp. 194-195, Montreal, Canada, 28 May- 1 Jun. 2001.

[10] *Alexa Top Global Sites*, http://www.alexa.com/topsites

[11] W. Lu, G. Rammidi, and A. Ghorbani, "Clustering botnet communication traffic based on n-gram feature selection," *Computer Communications*, vol. 34, no. 3, pp. 502-514, Mar. 2011.

[12] J. A. Pardo, L. Pardo, and M. C. Pardo, "The jensen-shannon divergence," *J. of the Franklin Institute*, vol. 334, no. 2, pp. 307-318, Mar. 1997.

[13] J. L. Myers and A. D. Well, *Research Design and Statistical Analysis*, New York, NY: Lawrence Erlbaum Associates, 2003.

[14] Q. Cheng, X. Chen, C. Xu, J. Shi, and P. Liu, "A bigram based real time DNS tunnel detection approach," in *Proc.of Int. Conf. on Information Technology and Quantitative Management*, vol. 17, pp. 852-860, China, May 2013.

[15] L. Wang, Y. Zhang, and J. Feng, "On the euclidean distance of images," *IEEE Trans. on Pattern Analysis and Machine Intelligence,* vol. 27, no. 8, pp. 1334-1339, Jun. 2005.

[16] P. N. Tan, M. Steinbach, and V. Kumar, *Introduction to Data Mining*, Boston, MA: Addison-Wesley, 2005.

[17] Open Malware, Community Malicious Code Research and Analysis, http://www.offensivecomputing.net

[18] GeoIP API, MaxMind, Open source API and Database for Geological Information, http://dev.maxmind.com/geoip/geoip2/geolite2

رضا شریف‌نیای دیزبنی در سال ۱۳۸۶ مدرک کارشناسی علوم کامپیوتر خود را از دانشگاه تبریز و در سال ۱۳۹۲ مدرک کارشناسی ارشد مهندسی کامپیوتر خود را از دانشگاه تربیت مدرس تهران دریافت نمود. نام‌برده از سال ۱۳۹۲ در معاونت تربیت و آموزش دانشگاه امام علی (ع) مشغول به فعالیت گردید و هم‌زمان نیز به عنوان استاد دروس کامپیوتر در دانشکده مهندسی و پرواز آن دانشگاه مشغول به کار بوده است. زمینه‌های تحقیقاتی مورد علاقه ایشان عبارتند از: تشخیص بدافزارها، امنیت شبکه، امنیت در وب و شبکه‌های کامپیوتری.

آناهیتا منافی مورکانی تحصیلات خود را در مقطع کارشناسی مهندسی کامپیوتر در سال ۱۳۹۰ از دانشگاه اصفهان و مقطع کارشناسی ارشد مهندسی کامپیوتر در سال ۱۳۹۲ از دانشگاه تربیت مدرس تهران به پایان رسانده است و هم اکنون به عنوان تحلیلگر ترافیک شبکه در شرکت دوران مشغول به کار می‌باشد. زمینه‌های علمی مورد علاقه نام‌برده شامل موضوعاتی مانند تجزیه و تحلیل ترافیک شبکه، تشخیص بدافزارها، امنیت در شبکه و ایده‌های نو در سخت افزارهای شبکه می‌باشد.