فصلنامه علمی-ترویجی پدافند غیرعامل
سال هفتم، شماره ۳، پاییز ۱۳۹۵، (پیاپی ۲۷): صص ۲۷-۱۹

تشخیص بات‌نت به‌وسیله تحلیل فعالیت‌های گروهی و پاسخ‌های ناموفق ترافیک شبکه

وحید محمدی[۱]، عباسعلی رضائی[*۲]

تاریخ دریافت: ۱۳۹۴/۰۶/۰۲
تاریخ پذیرش: ۱۳۹۴/۱۲/۱۰

چکیده

یکی از تهدیدات روزافزون در اینترنت و شبکه‌های کامپیوتری بات‌نت‌ها هستند. بات‌نت، شبکه‌ای از کامپیوترهای آلوده متصل به اینترنت است که تحت کنترل سرور فرماندهی و کنترل قرار می‌گیرد و برای حملات اینترنتی همچون حملات ممانعت از سرویس و فرستادن هرزنامه، مورد استفاده قرار می‌گیرد. بات‌نت با شناسایی دستگاه‌های آسیب‌پذیر موجود در شبکه و به مصالحه درآوردن آن‌ها، حیطه تحت کنترل خود را گسترش می‌دهد. بات‌نت‌ها به‌سرعت در حال پیشرفت هستند و از فنّاوری‌های جدید همچون DNS و تغییرات پی‌درپی سریع، برای به دام انداختن کاربران و افزایش حفاظت از کامپیوترهای آلوده خود بهره می‌برند. یکی از انواع تغییرات پی‌درپی سریع، استفاده از الگوریتم تولید نام دامنه است. مهاجمین با استفاده از این روش از قرار گرفتن نام دامنه سرویس‌دهنده‌های فرماندهی و کنترل خود در فهرست‌های سیاه جلوگیری می‌نمایند. بسیاری از روش‌های تشخیص بات‌نت، مبتنی بر تحلیل فعالیت گروهی بات‌نت‌ها هستند، اما استفاده از این روش به‌تنهایی، در شبکه‌های کوچک و متوسط کارایی مناسبی ندارد. هدف ما در این مقاله ارائه روشی جامع و کامل برای تشخیص بات‌نت‌هایی است که از تغییرات پی‌درپی نام دامنه در ترافیک استفاده می‌کنند و به‌صورت الگوریتمی تولید می‌شوند. روش ما قابلیت تشخیص بات‌نت‌های شناخته‌شده و همچنین ناشناخته‌ای که از این روش استفاده می‌کنند را دارا هست. در این روش، تشخیص بات‌نت‌ها بر اساس پاسخ‌های ناموفق یا NXDomain در هر میزبان صورت می‌گیرد. این ویژگی باعث می‌شود که دقت تشخیص در شبکه‌های کوچک و متوسط افزایش یابد. این روش در شبکه‌های آلوده به بات‌نت‌های کانفیکر و کراکن آزمایش و اطلاعات به‌دست‌آمده از آن مورد تجزیه و تحلیل قرارگرفته است.

کلید واژه‌ها: بات‌نت، هرزنامه، DNS، تغییر پی‌درپی دامنه، الگوریتم تولید نام دامنه، Nxdomain

---

۱- دانشجوی کارشناسی ارشد، دانشگاه پیام نور
۲- استادیار، گروه مهندسی کامپیوتر و فناوری اطلاعات، دانشگاه پیام نور،(a_razaee@pnu.ac.ir)_ نویسنده مسئول

۱- مقدمه

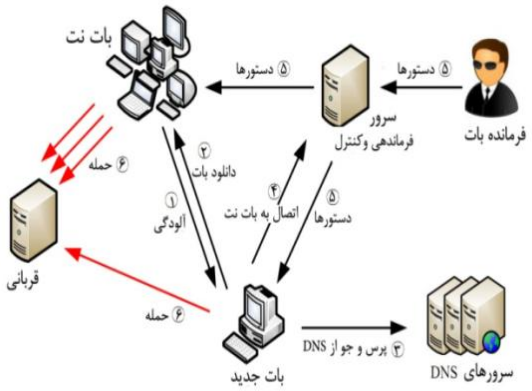
باتنت شبکه‌ای از ماشین‌آلات به خطر افتاده است که به‌وسیله مدیر بات[1] برای انجام حملات مورد استفاده و کنترل قرار می‌گردد [۱]. برخی حملات معمولی که باتنت‌ها در آن شرکت دارند شامل هرزنامه، فیشینگ و حملات ممانعت از سرویس توزیع‌شده[2] (DDOS) (DDOS) سرقت مشخصات کاربری و کلاه‌برداری یا تقلب از روی کلیک هست. با این حملات شبکه ها متحمل ضرر مالی قابل‌توجهی می‌شوند برای نمونه سالیانه تخمین‌زده‌شده که هرزنامه‌ها باعث ضرر و زیان سالانه ۲۰ میلیارد دلار آمریکا تنها در ایالت متحده شده است [۲].

کلمه بات که از روبات[3] گرفته‌شده بانام زامبی[4] نیز شناخته می‌شود مشابه روبات‌ها، از باتها برای انجام عملیات از پیش تعریف‌شده‌ای استفاده می‌شود که به‌صورت خودکار اجرا می‌شوند [۳]. اندازه یک باتنت به پیچیدگی و تعداد کامپیوترهای استخدام‌شده در این باتنت بستگی دارد. معمولاً کاربران کامپیوترها از این موضوع که دستگاه‌هایشان از راه دور کنترل‌شده و مورد سوءاستفاده قرار می‌گیرد اطلاعی ندارند. بر اساس مطالعاتی در سال ۲۰۰۷، حدود ۱۶ الی ۲۵ درصد از تمامی کامپیوترهای موجود بر روی اینترنت توسط باتنت‌ها آلوده بوده‌اند.

باتنت‌ها جهت جلوگیری از شناسایی شدنشان، سعی می‌کنند در مقیاس‌های بزرگی ایجاد شوند، یعنی تعداد کامپیوترهایی که به این گروه می‌پیوندند، زیاد هست همچنین اندازه باتنت یا تعداد میزبان‌های به مصالحه درآمده، عامل بالقوه‌ای را برای ارسال هرزنامه و حملات انکار سرویس توزیع‌شده، فراهم می‌کند [۴].

در قیاس باتنت با بدافزارهای موجود[5] (نرم‌افزارهای مخرب)، مانند کرم و ویروس، وجود کانال‌های فرماندهی و کنترل، تفاوت کلیدی است. زیرا باتنت‌ها تحت کنترل مهاجم دستور را دریافت و رفتارهای مخرب را انجام می‌دهند [۵]. با توجه به شکل (۱) مفاهیم مرتبط به باتنت، مثل فرمانده بات، سرور فرماندهی و کنترل، قربانی[6] و آلوده‌سازی نشان داده شده است.

1- Botmaster
2- Distributed Denial of Service(DDoS)
3- Robot
4- Zombie
5- Malware
6- Victom



شکل ۱. چرخه زندگی و ساختار یک باتنت بر پایه IRC [۶]

در چند سال اخیر تهدیدهای اینترنتی از انگیزه‌های فردی و سودجویی‌های مالی به حملات سایبری سازمان‌یافته به دولت‌ها و سازمان‌های دولتی گسترش‌یافته است. در اغلب این حملات از باتنت یا شبه باتنت‌ها در کنار سایر بدافزارها استفاده می‌گردد. باتنت‌ها توسط مهاجمان و از راه دور هدایت می‌شوند و اعضای آن‌ها در سراسر جهان وجود دارند. اخیراً از باتنت‌ها با اهداف سیاسی و نظامی و برای عملیات سایبری علیه زیرساخت‌های کشورها استفاده می‌شود. تعدادی از حملات سایبری خصوصاً علیه زیرساخت‌های کشورمان توسط باتنت‌ها یا شبه باتنت‌ها انجام‌شده است [۷]. با توجه به اهمیت موضوع باتنت و حملات سایبری که توسط این شبکه‌ها انجام می‌شود، امروزه بیش از پیش شناخت قابلیت‌های باتنت و ایجاد دستگاه‌هایی برای مقابله، تشخیص و کاهش اثرات آن‌ها موردتوجه قرار دارد. حمله‌کنندگان برای دشوار کردن عمل ردگیری و تشخیص باتنت به فنّاوری‌های جدیدی روی آورده‌اند، بنابراین باید متناسب با پیچیده شدن باتنت‌ها، روش‌های مقابله و تشخیص نیز ارتقاء یابند. یکی از دشواری‌های کشف باتنت در ترافیک واقعی وزنده، حجم بالای ترافیک واقعی و شباهت ترافیک باتنت به ترافیک نرمال شبکه است. در مواردی هم که ارتباطات باتنت رمز شده است بر دشواری‌های کشف می‌افزاید. تاکنون رویکردهای کشف بسیاری پیشنهادشده است که تمامی آن‌ها نیاز به تحلیل محتوای ترافیک باتنت دارند، اما رویکردهای پیشنهادی کشف هرکدام در زمینه‌ای خاص فعالیت می‌کنند. به دلیل گستردگی شبکه‌های باتنت و استفاده از فناوری و فن‌های متفاوت، ارائه یک‌راه حل جامع و کلی برای کشف شبکه‌های باتنت کار بسیار دشواری است. روش‌های کشف باتنت به دودسته کلی تقسیم می‌شوند، دسته اول بر اساس پروژه هانی نت[7] هست. دسته دوم، روش کشف باتنت بر اساس بررسی و تحلیل ترافیک غیرفعال شبکه است که خود به چهار دسته تقسیم می‌گردد:

7- Honynet

۱. دستگاه‌های کشف مبتنی بر امضا[1]:

فن‌های تشخیص مبتنی بر امضا را می‌توان برای تشخیص باتنت‌های شناخته‌شده استفاده نمود؛ بنابراین، این راه‌حل برای باتنت‌های ناشناخته و جدید کارایی ندارد.

۲. دستگاه‌های مبتنی بر رفتارهای غیرعادی[2]:

فن‌های مبتنی بر تشخیص رفتار غیرعادی سعی دارند باتنت‌های مبتنی بر ناهنجاری‌های متعدد ترافیک شبکه را کشف کنند، مانند بالا بودن تأخیر شبکه، حجم بالای ترافیک، ترافیک در پورت‌های غیرمعمول و رفتار غیرعادی سیستم که می‌تواند نشان‌دهنده بات‌های مخرب در شبکه باشد.

۳. دستگاه‌های مبتنی بر DNS[3]:

فن‌های تشخیص مبتنی بر DNS شبیه به الگوریتم‌های فن تشخیص مبتنی بر رفتار غیرعادی هستند که به بر روی ترافیک DNS عمل می‌کنند. بات‌ها به‌طورمعمول برای ارتباط با سرور فرماندهی و کنترل اقدام می‌کنند تا دستورات را دریافت نمایند. به‌منظور دسترسی به سرور فرماندهی و کنترل بات‌ها از DNS پرس‌وجو می‌نمایند تا سرور فرماندهی و کنترل مربوطه تعیین محل شود که به‌طورمعمول توسط ارائه‌دهنده DDNS میزبانی می‌شود؛ بنابراین، تشخیص ترافیک DNS باتنت توسط نظارت بر DNS و تشخیص ناهنجاری‌های ترافیک DNS امکان‌پذیر است.

۴. دستگاه‌های مبتنی برداده کاوی[4]:

چندین فن داده‌کاوی ازجمله یادگیری ماشین، طبقه‌بندی و دسته‌بندی را می‌توان به‌طور مؤثر برای شناسایی ترافیک فرماندهی و کنترل باتنت مورداستفاده قرارداد. بسیاری از باتنت‌های امروزی از فن‌هایی استفاده می‌کنند تا از روش‌های تشخیص سنتی بگریزند. در ادامه به یکی از این فن‌ها بنام الگوریتم تولید نام دامنه[5] اشاره می‌کنیم [۵ و ۸].

۲- مفاهیم مرتبط با سیستم DNS

سیستم نام دامنه یا DNS عنصری حیاتی از زیرساخت اینترنت است که برای ترجمه نام دامنه به آدرس IP مورداستفاده قرار می‌گیرد. بسیاری از سرویس‌های شبکه و برنامه‌های کاربردی مبتنی بر DNS هستند. سیستم نام دامنه قادر نیست که سرویس‌های آلوده را از سرویس‌های عادی تفکیک نماید، به همین دلیل بسیاری از بدافزارها ازجمله باتنت‌ها نیز از امکانات آن استفاده می‌کنند. بنابراین، می‌توان با نظارت بر DNS و تحلیل ترافیک آن، فعالیت باتنت‌ها را تشخیص داد. در این بخش مفاهیم مرتبط با DNS با تفصیل بیشتری مطرح می‌گردد .

۲-۱- الگوریتم تولید نام دامنه

باتنت‌ها برای گریز از دستگاه‌های تشخیص، از فناوری‌های مختلفی بهره می‌برند. آن‌ها ممکن است کانال‌های ارتباطی رمز شده مابین سرورهای فرماندهی و کنترل و بات‌ها ایجاد کنند، یا پیام‌های ارتباطی را از طریق شبکه‌های اجتماعی یا با استفاده از پنهان‌نگاری مخفی سازند. یکی دیگر از روش‌های گریز از دستگاه‌های تشخیص، فن تغییرات پی‌درپی سریع است که به دو نوع تقسیم‌بندی می‌شود. در نوع اول، فن تغییرات پی‌درپی سریع آدرس IP، چند آدرس IP، به یک نام دامنه نگاشت پیدا می‌کنند.

و در نوع دوم که فن تغییرات پی‌درپی سریع نام دامنه هست چند نام دامنه به یک آدرس IP اختصاص می‌یابند. باتنت‌های اخیر مثل Conficker، Kraken و Torping از تغییرات پی‌درپی نام دامنه مبتنی بر DNS برای فرماندهی و کنترل[6] بهره می‌برند. روشی که شاید ابتدا از Conficker شروع شد، اکنون در باتنت‌های مهمی نظیر Zeus هم دیده‌شده و به‌طور یقین در بدافزارهای بیشتری مورداستفاده قرار خواهد گرفت. نمونه‌ای از دامنه‌های تولیدشده توسط باتنت Kraken:

fvkvwf.dynserv.com

natiouwx.dyndns.org

afmbtgyktty.yi.org

در شبکه‌های باتنت که مبتنی بر تغییرات پی‌درپی سریع نام دامنه هستند، اعضای شبکه یعنی بات‌ها با تولید لیستی از نام‌های دامنه، رکورد A مربوط به این نام‌های دامنه موجود در لیست را به ترتیب مورد درخواست قرار می‌دهند تا درنهایت یکی از این نام‌های دامنه به یک آدرس IP، نگاشت یابد. خصوصیتی که نام‌های دامنه مبتنی بر این فن دارند این است که چون چند نام دامنه به یک آدرس IP نگاشت داده می‌شوند، این نام‌های دامنه در آدرس IP نگاشت داده‌شده، اشتراک دارند. این نام‌های دامنه مدت کوتاهی طول عمر دارند و از این ویژگی نیز می‌توان برای تشخیص آن‌ها استفاده نمود. برای محاسبه دامنه‌های جدید، یک الگوریتم تولید نام دامنه یا به اختصار DGA به‌کار برده می‌شود [۹]. برای مقابله با باتنت‌هایی که از فن تغییرات پی‌درپی نام دامنه استفاده می‌کنند،

1- Signature-based Detection
2- Anomaly-based Detection
3- DNS-based Detection
4- Mining-based Detection
5- Domain Name Generation Algorithm(DGA)
6- Command and Control

الگوریتم تولید نام دامنه باید شناخته شود. فرماندهان بات از الگوریتم‌های تولید نام دامنه برای تولید پویای تعداد زیادی از نام‌های دامنه تصادفی استفاده می‌نمایند و زیرمجموعه کوچکی از آن را برای فرماندهی و کنترل واقعی استفاده می‌کنند. به‌عبارت‌دیگر، یک دامنه فرماندهی و کنترل به‌صورت تصادفی تولیدشده و برای دوره زمانی بسیار کوتاهی استفاده می‌شود، بنابراین رویکردهای تشخیصی که وابسته به لیست دامنه ایستا هستند (لیست سیاه) غیر مؤثر خواهند شد. بدیهی است که اگر بدانیم که الگوریتم تولید دامنه چگونه کار می‌کند، می‌توانیم دامنه‌ها را پیش از زمان تولید نماییم و ترافیک فرماندهی و کنترل بات‌نت را مسدود کنیم [۶].

ورودی یکسان تضمین می‌کند که بات های عضو یک بات‌نت، نام‌های دامنه‌ی یکسانی تولید می‌کند. اکثر سرویس‌دهنده‌های امن از نام‌های دامنه‌ای استفاده می‌کنند که کاربران بتوانند آن نام‌ها را به‌راحتی به خاطر بسپارند .به‌عنوان‌مثال، نام دامنه‌ی مربوط به بانک ملت به‌صورت www.bankmellat.ir هست؛ اما در بات‌نت‌ها این موضوع چندان از اهمیت برخوردار نیست .درواقع، مهاجمین باید نام‌های دامنه‌ی سرویس‌دهنده‌های فرمان و کنترل را طوری ایجاد کنند که در صورت استفاده از روش‌های تغییر پی‌درپی دامنه، مشابه نام‌های دامنه‌ی ثبت‌شده توسط سرویس‌دهنده‌های امن نباشند . به‌طورمعمول، در دنیای واقعی ترکیب حروف نام‌های دامنه‌ای که توسط این الگوریتم‌ها ایجاد می‌شوند، مورداستفاده قرار نمی‌گیرند . به‌عنوان‌مثال، نام دامنه‌ی tvxwoajfwad.info توسط Conficker-C ایجاد می‌شود که چون به‌صورت الگوریتمی ایجادشده است، هیچ معنای خاصی ندارد. جهت شناسایی نام‌های دامنه‌ی تولیدشده، ابتدا باید نحوه‌ی عملکرد الگوریتم تولید نام دامنه مشخص شود .بدین منظور، می‌توان کد باینری [1] بات را اجرا کرده و با مهندسی معکوس آن را شناسایی کرد .انجام این کار به هزینه و زمان زیادی نیاز دارد. همچنین، مهاجم می‌تواند ورودی الگوریتم را در دستورات جدید عوض کند .بنابراین، با صرف هزینه‌ی زیاد هم ممکن است نتوان ورودی این الگوریتم‌ها را شناسایی کرد .این عوامل باعث شده که استفاده از روش‌های تغییر پی‌درپی دامنه از محبوبیت زیادی در بات‌نت‌های نسل جدید برخوردار باشند [۱۰]. استفاده از الگوریتم تولید نام‌های دامنه برای تغییر پی‌درپی دامنه، روشی است که ابتدا از بدافزار Conficker شروع شد؛ اما اکنون در بدافزارهای مخرب و مهمی نظیر Zeus هم دیده‌شده و به‌طور یقین در بدافزارهای بیشتری مورداستفاده قرار خواهد گرفت .همین امر باعث شده است تا تولیدکنندگان محصولات امنیتی به فکر چاره‌اندیشی باشند .به همین دلیل، تحقیقات در این زمینه با توجه به پیچید ه تر شدن این الگوریتم‌ها روزبه‌روز بیشتر می‌شود [۱۱].

استفاده از روش‌های تغییر پی‌درپی دامنه یا الگوریتم تولید نام دامنه از می‌توان نام‌های دامنه الگوریتمی را با نظارت بر ترافیک DNS شناسایی نمود زیرا ویژگی‌های ترافیک DNS در این نوع بات‌نت‌ها پایدار بوده و به‌راحتی قابل‌تغییر یا جایگزینی نیست. بسیاری از محققان معتقدند که تحلیل DNS روشی مؤثر برای تشخیص بات‌نت‌ها است، به‌خصوص برای آن‌هایی که دارای رفتار تغییرات پی‌درپی دامنه هستند. مزیت تحلیل ترافیک DNS این است که به حجم کمی از ترافیک شبکه نیاز دارد، به محتوای ترافیک و امضاهای شناخته‌شده نیازی ندارد و نیز ارتباطات رمزشده را تشخیص می‌دهد. این روش مستقل از پروتکل و ساختار است و می‌تواند بات‌نت‌ها را در مراحل آغازین و قبل از وقوع حمله شناسایی کند [۶].

۲-۲- تجزیه و تحلیل کارهای مرتبط

برای تشخیص بات‌نت‌ها روش‌های مختلفی پیشنهادشده است که در ادامه به برخی از آن‌ها اشاره می‌شود:

Choi و همکاران [۱۲ و ۱۳] روشی به نام BotGAD پیشنهاد کردند که بر اساس نظارت بر فعالیت‌های گروهی[2] ترافیک DNS عمل می‌کند. آن‌ها در ابتدا ویژگی فعالیت گروهی ترافیک DNS را به‌عنوان ویژگی کلیدی بات‌نت تعریف کردند و بر اساس آن ترافیک معمولی DNS را از ترافیک DNS بات‌نت‌ها متمایز نمودند. ازآنجا که ترافیک DNS در چند مرحله از چرخه زندگی بات‌نت ظاهر می‌شود، بنابراین با استفاده از خصوصیت فعالیت گروهی، می‌توان بات‌نت را تشخیص داد. چارچوب BotGAD شامل پنج بخش اصلی است: جمع‌آوری‌کننده داده، نگاشت دهنده داده، استخراج‌کننده دامنه‌های همبسته، تولیدکننده ماتریس و تحلیل‌گر شباهت.

آن‌ها روش تشخیص بات‌نت مبتنی بر ناهنجاری را ارائه کرده‌اند که با نظارت بر فعالیت‌های گروهی در ترافیک DNS، بات‌نت‌ها را در مراحل مختلف از چرخه حیات آن‌ها تشخیص می‌دهد. این فعالیت گروهی بر اساس پرس‌وجوهای DNS ارسال‌شده به‌صورت همزمان توسط بات‌های توزیع‌شده شکل می‌گیرد. در این روش، از ویژگی‌های متمایزکننده بین پرس‌وجوهای DNS بات‌نت برای تشخیص استفاده می‌شود. این روش بسیار مؤثرتر از روش‌های قبلی عمل می‌کرد. این روش مستقل از ساختار و پروتکل بود و همچنین می‌توانست بات‌نت‌هایی را تشخیص دهد که کانال رمزشده داشتند. بااین‌حال، ضعف اصلی این رویکرد، صرف زمان پردازش زیاد برای نظارت بر شبکه‌های با مقیاس بزرگ بود. همچنین این روش تنها قادر به

1- Binary Code

2- Group Activity Property

تشخیص باتنت‌هایی است که در مراحل مختلف از چرخه حیات خود از درخواست DNS استفاده می‌کند. اگر باتنت‌های عضو یک باتنت تنها در مرحله شکل‌گیری از پرس‌وجوهای DNS استفاده کرده و یا از محبوبیت زیادی در باتنت‌های نسل جدید برخوردار باشند.

آدرس‌های IP به‌جای نام‌های دامنه استفاده کنند. روش فوق قادر به تشخیص آن باتنت نخواهد بود. استفاده از این روش به‌تنهایی، در شبکه‌های کوچک و متوسط کارایی مناسبی ندارد.

رماچندران و همکارانش در [۱۴] از فهرست سیاه نام دامنه (DNSBL) برای شناسایی باتنت‌های ارسال‌کننده هرزنامه، استفاده کردند. ایده روش این است که مدیر بات برای اطلاع از وضعیت مسدود شدن آدرس IP باتها، از فهرست سیاه DNS پرس‌وجو می‌کند. با توجه به این نکته که تعداد این پرس‌وجوها از طرف مدیر بات زیاد است، مدیر بات را شناسایی می‌کند. این روش خطای مثبت زیادی دارد.

GU و همکاران [۱۵ و ۱۶] یک روش مبتنی بر خوشه‌بندی برای تشخیص باتنت‌ها 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 دستگاه‌های تشخیص باتنت یک ضعف عمده است. این پژوهش بر مبنای روش چوی و همکاران، ۲۰۰۹ متمرکز شده است.

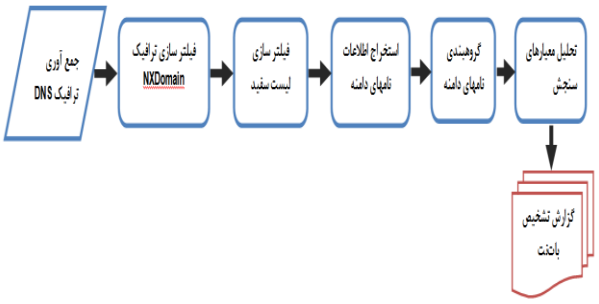
۳- ساختار سیستم پیشنهادی تشخیص باتنت

روش پیشنهادی ما ضعف‌های روش‌های مذکور را برطرف و خصوصیاتی از ترافیک DNS و فعالیت باتنت‌های مبتنی بر الگوریتم تولید نام دامنه را مدنظر قرار خواهد داد که در هر میزبان به‌طور جداگانه قابل اندازه‌گیری باشد. در این روش، تشخیص باتنت‌ها بر اساس پاسخ‌های ناموفق یا NXDomain در هر میزبان صورت می‌گیرد. این ویژگی باعث می‌شود که دقت تشخیص در شبکه‌های کوچک و متوسط افزایش یابد. همچنین روش پیشنهادی مبتنی بر تحلیل ترافیک DNS بوده و دارای مزایای زیر هست:

به ترافیک کم‌حجم DNS نیاز دارد و درنتیجه سرعت پردازش سیستم افزایش می‌یابد. تشخیص باتنت قبل از اجرای حمله یا همان مراحل ابتدایی امکان‌پذیر است. باتنت‌های شناخته‌شده و همچنین ناشناخته‌ای که از این روش استفاده می‌کنند را تشخیص داده، به امضاء و فهرست سیاه نیازی ندارد. این روش مستقل از پروتکل و ساختار باتنت است و به تحلیل محتوای بسته‌ها نیازی ندارد.

با توجه به اینکه DNS یکی از رایج‌ترین پروتکل‌ها در شبکه است و برای کارکرد صحیح فعالیت‌های زیادی در شبکه‌ها ضروری است. به همین دلیل DNS برای مانیتورینگ[1]، تشخیص و کاهش فعالیت باتنت‌ها 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.

در شکل (۲)، ساختار سیستم پیشنهادی ارائه شده است. روش پیشنهادی شامل هفت مؤلفه اصلی هست که عبارت‌اند از جمع‌آوری ترافیک DNS، فیلترسازی ترافیک NXDOMAIN، فیلترسازی فهرست سفید، استخراج اطلاعات نام‌های دامنه، گروه‌بندی نام‌های دامنه، تحلیل معیارهای سنجش و گزارش تشخیص باتنت؛ که مؤلفه‌های مختلف این سیستم در این مقاله به‌طور کامل تشریح می‌گردد.



شکل ۲. ساختار سیستم تشخیص باتنت پیشنهادی

۳-۱- جمع‌آوری ترافیک DNS

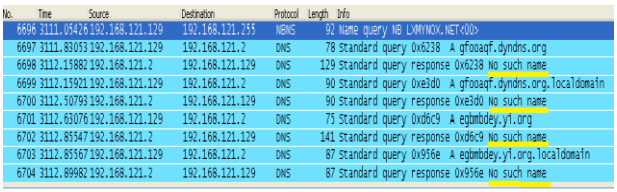
سیستم پیشنهادی در سرویس‌دهنده DNS یا در لبه شبکه قرار می‌گیرد تا درخواست‌های DNS ماشین‌های داخل شبکه و پاسخ‌های دریافتی را ثبت و نظارت نماید. واضح است فقط ترافیک DNS مدنظر است که درصد کمی از ترافیک کل شبکه هست. با توجه به فعالیت روزانه باتنت‌های مبتنی بر الگوریتم نام دامنه، فرض بر این است که این نوع از بات ها حداقل روزی یک‌بار اجرا می‌شوند؛ بنابراین حداکثر دوره زمانی برای جمع‌آوری ترافیک ۲۴ ساعت خواهد بود.

۳-۲- فیلترسازی ترافیک NXDomain

در شبکه‌های بات، اعضای شبکه سعی در برقراری ارتباط با سرور فرماندهی و کنترل[2] دارند تا دستورات حمله را دریافت نمایند، به همین دلیل شروع به فرستادن درخواست‌های رکورد A به سیستم

1-Monitoring
2-Server command and control

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 NXDomain باشند و مابقی ترافیک DNS حذف خواهد شد؛ بنابراین بازهم حجم ترافیک ورودی به سیستم تشخیص کاهش خواهد یافت. همان‌طور که اشاره گردید، یکی از ویژگی‌های کلیدی بات‌نت‌های مبتنی بر الگوریتم تولید نام دامنه، تولید روزانه نگاشت‌های ناموفق یا NXDomain ها برای نام‌های دامنه‌ای است که وجود ندارند؛ بنابراین در میزبانی که به بات آلوده است تعداد NXDomainها نسبت به میزبان‌های عادی به‌طور قابل‌توجهی بیشتر است NXDomainها غالباً به‌صورت گروهی تولید می‌شوند؛ بنابراین در ترافیک شبکه‌ای که آلوده به بات‌های 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 Aو پاسخ‌های ناموفق در ترافیک DNS بات‌نت کراکن مشاهده می‌شود. این ترافیک از طریق اجرای کد بات کراکن بر روی یک میزبان متصل به اینترنت به‌دست آمده است.



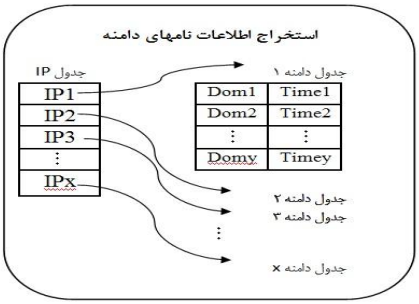
شکل ۳. فعالیت بات‌نت کراکن و پاسخ‌هایNXDomain

۳-۳- فیلترسازی فهرست سفید

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 حذف شده 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 [۱۷] مورد استفاده قرار می‌گیرد. به این دلیل که صد سایت پربازدید در اینترنت به‌احتمال زیاد به بات آلوده نیستند.

۴-۳- استخراج اطلاعات نام‌های دامنه

پس از اعمال فیلترهای مختلف روی ترافیک DNS، ترافیک باقیمانده، فقط شامل درخواست‌های رکورد A فاقد پاسخ بوده و دامنه‌های معتبر در آن موجود نیستند؛ بنابراین در مؤلفه استخراج اطلاعات نام‌های دامنه، هر میزبانی که اولین بار درخواست رکورد A فاقد پاسخ یا NXDomain داشته باشد، آدرس IP آن در جدول IP ثبت می‌شود، سپس جدول دامنه مربوط به IP مذکور تشکیل‌شده و در آن نام‌های دامنه و زمان درخواست رکورد A مربوط به آن IP ثبت می‌شوند. این اطلاعات در مراحل بعدی برای گروه‌بندی نام‌های دامنه و تحلیل معیارهای سنجش مورداستفاده قرار خواهند گرفت. مؤلفه استخراج اطلاعات نام‌های دامنه در شکل (۴) مشاهده می‌شود.



شکل ۴. استخراج اطلاعات نام‌های دامنه

۵-۳- گروه‌بندی نام‌های دامنه

با بررسی ترافیک شبکه عادی و نیز شبکه آلوده به بات مشاهده می‌گردند که تعداد پاسخ‌های NXDomain در میزبان‌های آلوده بسیار بیشتر از میزبان‌های عادی است. با استفاده از این موضوع، تعداد پاسخ‌های NXDomain در یک دوره زمانی محاسبه می‌گردد و آن‌هایی که از یک حد آستانه بیشتر باشند گروه‌بندی می‌شوند [۱۲]. میزبان‌های مختلف می‌توانند مجموعه‌ای از نام‌های دامنه تولید نمایند که اولا به IP مشابه نگاشت شوندو ثانیا دارای TLD[1] یا SLD[2] یکسان باشند. معمولاً گروه‌بندی نام‌های دامنه بر اساس یکی از موارد فوق یا ترکیبی از آن‌هاست. درروش پیشنهادی با توجه به فعالیت روزانه بات‌نت‌های مبتنی بر الگوریتم تولید نام دامنه، در یک مقطع زمانی (حداکثر یک روز) فعالیت‌های موردنظر هر میزبان درخواست‌کننده ثبت‌شده و پس از استخراج اطلاعات نام‌های دامنه گروه‌بندی بر اساس TLD یا SLD مشترک در هر میزبان انجام خواهد شد. در جدول (۱) نمونه‌ای از گروه‌بندی نام‌های دامنه بر اساس TLD و SLD یکسان نمایش داده‌شده است. در بخش تحلیل معیارهای سنجش، از اطلاعات گروه‌بندی نام‌های دامنه استفاده خواهد شد.

1- Top Level Domain
2- Second Level Domain

جدول ۱. گروه‌بندی نام‌های دامنه

گروه‌بندی بر اساس SLD مشابه	گروه‌بندی بر اساس TLD مشابه
evnmcjcbj.mooo.com	cuqpwpmhbe.org
yyxrelchaix.mooo.com	sucizpc.org
uvsbzwy.mooo.com	mwolcungru.org
rhpstjtlwdm.mooo.com	yknpotrh.org

انجام محاسبات و تحلیل معیارهای سنجش: از اطلاعات دریافتی از مؤلفه‌های قبلی و با انجام محاسباتی بر روی جدول نام دامنه برای هر IP یا میزبان معین، می‌تواند سه معیار تعریف نمود. معیارها عبارتنداز 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.

۳-۶- 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 بات‌نت‌های مبتنی بر تولید نام دامنه حداکثر برابر ۲۴ ساعت خواهد بود. در میزبانی که به بات آلوده است تعداد NXDomainها 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 زمانیT

ب-تراکم درخواست‌های رکورد[1]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 (۱) به دست آورد:

$$p = \sum_{i=1}^{n-1}(t_{i+1} - t_i)/n-1) \qquad (۱)$$

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.

1-Record

ج- معیار گروه‌بندی: با توجه به تولید تعداد زیاد نام‌های دامنه شبه تصادفی در بات‌نت‌های مبتنی بر الگوریتم تولید نام دامنه، احتمال ایجاد گروه‌های نام دامنه بسیار زیاد است .مجموعه‌ای از نام‌های دامنه در صورتی یک گروه هستند که حداقل دارای دو عضو باشند؛ بنابراین در گروه‌بندی ما، دامنه‌های تک عضوی در نظر گرفته نمی‌شوند .ازگروهبندی نام‌های دامنه می‌توان اطلاعات زیر را به دست آورد:

تعداد گروه‌های تشکیل‌شده در یک میزبان معین در دوره زمانی Tرا با متغیر N_gنشان می‌دهیم .همچنین تعداد اعضای گروه k را با M_k نشان می‌دهیم. آنگاه معیار گروه‌بندی را با رابطه (۲) زیر تعریف می‌کنیم.

$$g=\sum_{k=1}^{n_g}(m_k)/n \qquad 0 \le g \le 1 \qquad (۲)$$

بدترین حالت برای گروه‌بندی زمانی است که هیچ‌یک از نام‌های دامنه عضو مشابهی نداشته باشد و هیچ گروهی تشکیل نشود. در این حالتM_k برابر با صفر شده و درنتیجه معیار گروه‌بندی یعنی g نیز برابر صفر خواهد شد. بهترین حالت زمانی است که کلیه نام‌های دامنه در گروه‌بندی مشارکت داشته باشند. در این حالت، مجموع اعضای گروه برابر n شده و درنتیجه معیار گروه‌بندی یعنی g نیز برابر یک خواهد شد.

۳-۷ -گزارش تشخیص بات‌نت

اگر گروه‌بندی از حد آستانه‌ای بیشتر باشد نشان‌دهنده وجود بات هست. 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.

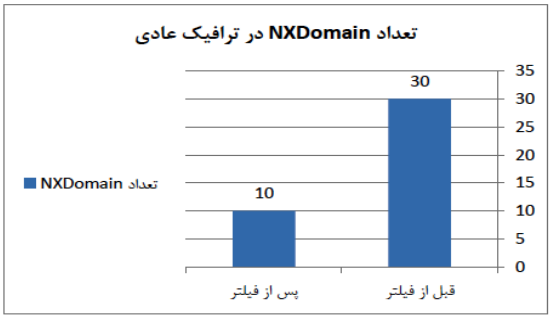
۴- نتایج آزمایش

فایل‌های اجرایی کانفیکر و کراکن که از نوع بات‌نت‌های مبتنی بر نام دامنه هستند از اینترنت دانلود و روی چند سیستم مجازی اجرا گردیدند. با استفاده از نرم‌افزار وایرشارک [۱۲] [2] و تحت سیستم‌عامل ویندوزxp، ترافیک بات‌نت‌های 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 همچنین در موارد متعدد و در ساعات

1- wireshark

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 NXDomain ها 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 Tمحاسبه شد .قبل از فیلتر n = ۳۰ و پس از فیلتر n = ۱۰ به دست آمد. این موضوع در نمودار شکل ۵ مشاهده می‌شود.



شکل ۵. نمودار تعدادNXDomain

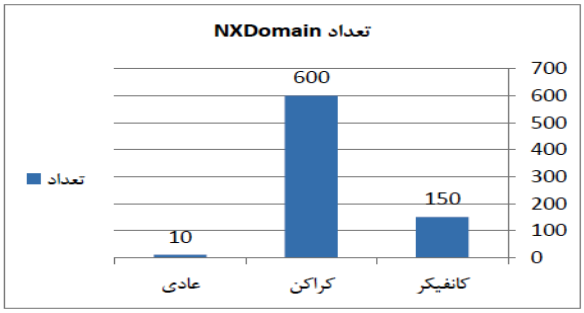
مواردی که فیلتر شده‌اند عبارت‌اند از درخواست‌های تکراری، درخواست‌های غیر از رکورد A یا درخواست‌های موجود در فهرست سفید بوده است. در جدول (۲) مواردی از ترافیک DNS نشان داده شده است، این درخواست‌ها، غیر از رکورد A بوده‌اند و به همین دلیل فیلتر شده‌اند.

جدول ۲. پاسخ‌های NXDomain - فیلترشده

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[1]، کراکن[2] و ترافیک عادی با یکدیگر مقایسه شده است. مطابق نمودار شکل (۶)، تعداد NXDomainها در میزبان‌های آلوده بسیار بیشتر از میزبان‌های عادی است.

1-Conficker
2-Kracken



شکل ۶. نمودار تعدادNXDomain

حد آستانه‌ای به نام NXDomain تعریف نموده و میزبان‌هایی که بیش‌ازحد آستانه α دارند، در مرحله بعد گروه‌بندی می‌شوند و از بررسی سایر میزبان‌ها صرف‌نظر می‌شود. با استفاده از نتایج به‌دست‌آمده از 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. در جدول (۳) متوسط فاصله زمانی بین درخواست های رکورد A آورده شده است.

جدول ۳. متوسط فاصله زمانی بین درخواست‌های رکورد A

نوع ترافیک	γ
کانفیکر	۸
کراکن	۳
عادی	>۱۰

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

بررسی معیار گروهی بودن: لازم به توضیح است در گروه‌بندی نام‌های دامنه باتنت کانفیکر، ۵ گروه بر اساس TLD مشابه تشکیل گردید که TLD های مربوطه عبارت‌اند از: com، org، cc، net و . info در گروه‌بندی نام‌های دامنه باتنت کراکن، ۴ گروه بر اساس SLD مشابه تشکیل گردید که SLD های مربوطه عبارت‌اند از: dyndns، yi، mooo و dynserv. ۳ گروه نیز بر اساس TLD مشابه ایجاد شد که عبارت‌اند از: com، org و net. در جدول (۴) معیار گروهی بودن باتنت های کانفیکر و کراکن آورده شده است. از جدول(۴) مشخص می‌شود که در فعالیت باتنت‌ها مقدارβ بیش از ۰/۸ است برای حد آستانه مقدار β= ۰/۵ را در نظر می‌گیریم؛ یعنی باید بیش از نیمی از نام‌های دامنه در گروه‌بندی مشارکت داشته

باشند تا شرط گروه‌بندی برای تشخیص باتنت محقق شود.

جدول ۴. معیار گروهی بودن باتنت‌های کانفیکر و کراکن

عنوان باتنت	n	N_g	g
کانفیکر	۱۵۰	۵	۰/۹۸
کراکن	۶۰۰	۷	۰/۸۰

۵- نتیجه‌گیری

در این مقاله، روشی جدید مبتنی بر شناسایی نام‌های دامنه الگوریتمی برای تشخیص باتنت‌های نسل جدید ارائه شد. که با توجه به اطلاعات و روابط به‌دست‌آمده می‌توان درباره آلوده بودن یا عادی بودن نام‌های دامنه یک میزبان معین در دوره زمانی T طبق شرایط زیر تصمیم گرفت:

اگر $n>\alpha$ و $g>\beta$ و $p<\gamma$ باشد آنگاه میزبان موردنظر آلوده به بات تشخیص داده می‌شود .همان‌طورکه ذکر گردید مقادیرα ، β و γ به ترتیب عبارت‌اند از ۱۰، ۰/۵ و ۱۰

در این مقاله روشی جامع و کامل برای تشخیص باتنت‌هایی که از تغییرات پی‌درپی نام دامنه در ترافیک استفاده می‌کنند و به‌صورت الگوریتمی تولید می‌شوند ارائه شده است. روش پیشنهادی قابلیت تشخیص باتنت‌های شناخته‌شده و همچنین ناشناخته‌ای که از این روش استفاده می‌کنند را دارا هست. در این روش، تشخیص باتنت‌ها بر اساس پاسخ‌های ناموفق یا NXDomain در هر میزبان صورت می‌گیرد. این ویژگی باعث می‌شود که دقت تشخیص در شبکه‌های کوچک و متوسط افزایش یابد.

۶- مراجع

1. M. Feily, A. Shahrestani, and S. Ramadass, “A Survey of Botnet and Botnet Detection,” in Proceedings of the 2009 Third International Conference on Emerging Security Information, Systems and Technologies, 2009, pp. 268–273.
2. Q. Lone, G. C. M. Moura, and M. Van Eeten, “Towards Incentivizing ISPs to Mitigate Botnets,” in Monitoring and Securing Virtualized Networks and Services: 8th IFIP WG 6.6 International Conference on Autonomous Infrastructure, Management and Security, AIMS 2014, Brno, Czech Republic, June 30– July 3, 2014. Proceedings, A. Sperotto, G. Doyen, S. Latré, M. Charalambides, and B. Stiller, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 57–62, 2014.
3. J. Vania, A. Meniya, and H. B. Jethva, “A Review on Botnet and Detection Technique,” vol. 4, no. 1, pp. 23–29, 2013.
4. K. Alieyan, A. ALmomani, A. Manasrah and M. M. Kadhum, “A survey of botnet detection based on DNS,” Neural Comput. Appl., pp. 1–18, 2015.
5. T. Barabosch, A. Wichmann, F. Leder, and E. Gerhards-Padilla, “Automatic Extraction of Domain Name Generation Algorithms from Current Malware,” NATO Symp. Inf. Assur. Cyber Def., pp. 1–13, 2012.
6. L. V. Hong, “DNS Traffic Analysis for Network-based Malware Detection DNS Traffic Analysis for Network-based Malware Detection,” p. 67, 2012.
7. M. Antonakakis and R. Perdisci, “From throw-away traffic to bots: detecting the rise of DGA-based malware,” Proc. 21st USENIX Secur. Symp., p. 16, 2012.
8. J. Park, “Acquiring Digital Evidence from Botnet Attacks: Procedures and Methods,” Communication, 2011.
9. T. S. Wang, C. S. Lin, and H. T. Lin, “DGA Botnet Detection Utilizing Social Network Analysis,” in 2016 International Symposium on Computer, Consumer and Control (IS3C), 2016, pp. 333–336.
10. D. Piscitello, “Conficker summary and review,” pp. 1–18, 2010.
11. M. A. Rajab, J. Zarfoss, F. Monrose, and A. Terzis, “My botnet is bigger than yours (maybe, better than yours): why size estimates remain challenging,” HotBots07 Proc. first Conf. First Work. Hot Top. Underst. Botnets, p. 5, 2007.
12. H. Choi and H. Lee, “Identifying botnets by capturing group activities in DNS traffic,” Comput. Networks, vol. 56, no. 1, pp. 20–33, 2012.
13. H. Choi, H. Lee, and H. Kim, “BotGAD: detecting botnets by capturing group activities in network traffic,” Proc. Fourth Int. ICST Conf. Commun. Syst. Softw. Middlew., pp. 1–8, 2009.
14. A. Ramachandran, N. Feamster, and D. Dagon, “Revealing Botnet Membership Using DNSBL Counter-Intelligence,” 2005.
15. G. Gu, R. Perdisci, J. Zhang, and W. Lee, “BotMiner: Clustering Analysis of Network Traffic for Protocol- and Structure-independent Botnet Detection,” in Proceedings of the 17th Conference on Security Symposium, 2008, pp. 139–154.
16. G. Gu, P. Porras, V. Yegneswaran, M. Fong, and W. Lee, “BotHunter: Detecting Malware Infection Through IDS-driven Dialog Correlation,” in Proceedings of 16th USENIX Security Symposium on USENIX Security Symposium, 2007, p. 12.
17. R. Sharifnya and M. Abadi, “A novel reputation system to detect DGA-based botnets,” in Computer and Knowledge Engineering (ICCKE), 2013 3th International eConference on, 2013, pp. 417–423.

Botnets Detection by Analyzing Network Traffic Group Activities and Unsuccessful Responses

V. Mohammadi, A. Rezaee*

Abstract

Botnets are one of the growing threats on the Internet and computer networks. Botnet is a network of infected computers connected to the Internet, which is controlled by a control server, and used for Internet attacks such as denial of service attacks, and spams. Botnets expand the their territory by identifying vulnerable devices on the network and get them to compromise. They are progressing rapidly and use new technologies such as DNS and quick continuous changes, to trap their users and enhance the protection of infected computers. One of the quick continuous changes is using a domain name generation algorithm. By using this method attackers prevent, control server domain names to be in black lists. Many Botnet detection methods are based on an analysis of group activity, but using this method alone does not have sufficient performance in small and medium networks. The aim of this paper is to provide a comprehensive and complete method to detect Botnets that use quick domain name changes algorithmivckly. Our method is capable of detecting Botnets that work in this way. In this method Botnets are detected based on failed responses or NXDomain in each host. This feature increase detection accuracy in small and medium networks. Our method is tested in infected networks with Conficker and Kraken and information obtained from them has been analyzed.

Key Words: *Botnets, Spam, DNS, The Continuous Change, Domain Name Generation Algorithm,Nxdomain*

* Payam Noor university (a_razaee@pnu.ac.ir) - Writer-in-Charge