فصلنامه علمی-ترویجی پدافند غیرعامل
سال هفتم، شماره ٤، زمستان ۱۳۹۵، (پیاپی ۲۸): صص ۳۲-۲۳

# پایش مشخصه‌های جریان‌های بات‌نتی با ارائه یک سامانه تحلیل ترافیک شبکه

مریم رحیمی‌پور[۱]، افشین فیروزی[۲]، شهرام جمالی[۳*]

تاریخ دریافت: ۱۳۹۴/۰۶/۱۱
تاریخ پذیرش: ۱۳۹۵/۰۶/۰۸

## چکیده

بات‌نت یکی از خطرات مهم ولی کمتر شناخته شده در اینترنت است. بات‌نت‌ها شبکه‌ای از کامپیوترهای تسخیر شده تحت کنترل هستند که از طریق یک کانال فرمان و کنترل برای حملاتی با قدرت تخریب بالا و وسعت زیاد هدایت می‌شوند. بات‌نت‌ها اغلب برای اقدامات خرابکارانه مهمی همچون حملات انکار سرویس توزیع شده مورد بهره‌برداری قرار می‌گیرند. برای مقابله با این نوع از حملات لازم است ساختار، ویژگی‌ها و رفتار ترافیکی بات‌نت به خوبی مورد بررسی قرار گیرد بنابراین شناسایی شاخصه‌های اصلی بات‌نت‌ها و مانیتورینگ جریان‌های بات‌نتی در ایجاد و توسعه تکنولوژی‌های مواجهه با این خطر امنیتی مهم، موثر خواهد بود. در این مقاله بات‌نت‌ها، چرخه حیات آنها و انواع توپولوژی و پروتکل‌های مورد بهره‌گیری آنها بررسی و با پیاده‌سازی یک شبکه آلوده به بات‌نت و ارائه سامانه آنالیز جریان شبکه، رفتارها و ویژگی‌های ترافیک بات‌نتی مستند می‌شود. با پیاده‌سازی این سامانه ویژگی‌های جریان‌ها و رفتار بات‌نتی به‌نحو مطلوبی نمایش داده شده است. مشاهده این ویژگی‌ها برای ارائه راه‌کارهای تشخیص مقابله با حملات مبتنی بر بات‌نت موثر خواهد بود.

**کلیدواژه‌ها:** بات‌نت، جریان، حمله، فرمان و کنترل

۱- کارشناسی ارشد مهندسی کامپیوتر- دانشگاه آزاد اسلامی واحد علوم و تحقیقات اردبیل
۲- کارشناس- مرکز فناوری اطلاعات و ارتباطات– اداره کل راه و شهرسازی استان اردبیل
۳- دانشیار- مهندسی کامپیوتر و فناوری اطلاعات- دانشگاه محقق اردبیلی، jamali@iust.ac.ir - نویسنده مسئول

## ۱- مقدمه

امروزه باتنت[1] به‌طور گسترده در حملات سایبری خطرناک، برای حمله به شبکه‌ها و دارایی‌های اطلاعاتی سازمان‌ها مورد استفاده قرار می‌گیرد. باتنت به بستر[2] اصلی و قابل توسعه‌ای برای حملات و اقدامات خرابکارانه تبدیل شده است و بیشتر انواع جدید حملات با استفاده از این بستر صورت می‌گیرد. بات‌ها جهت اجرای انواع گسترده‌ای از اقدامات مخرب و مجرمانه علیه سامانه‌ها و سرویس‌های آنها مورد استفاده قرار می‌گیرند. حملات DOS، انتشار اسپم[3]، فیشینگ و ... از جمله حملات قابل ترتیب توسط باتنت هستند [۱]. باتنت یا شبکه بات از تعداد زیادی از کامپیوترهای آسیب‌پذیر که توسط کدهای مخربی[4] مورد نفوذ قرار گرفته‌اند و به‌وسیله فرمان‌های ارسالی از راه دور از طریق اینترنت تحت ساختار فرمان و کنترل قابل کنترل و هدایت هستند [۲]. راه‌کارهای مختلفی برای مقابله با حملات مبتنی‌بر باتنت ارائه شده است اما این راه‌کارها به‌طور کامل نتوانسته‌اند از حملات باتنت ممانعت به‌عمل آورند. باتنت‌ها همواره هوشمندتر شده و از روش‌های جدیدتری برای مراحل مختلف خود بهره می‌برند. آنچه که در تمام باتنت‌ها مشترک است بهره‌گیری از ساختار فرمان و کنترل و رفتار ترافیکی تقریبا یکسان آنها است. در این میان راه‌کارهایی که نحوه عمل آنها مبتنی بر شناسایی رفتار و تجزیه و تحلیل ترافیک باتنت بوده است تقریبا موفق‌تر بوده و توانسته‌اند با بررسی و تحلیل رفتار ترافیکی در یک شبکه، باتنت‌ها را شناسایی نمایند. برای ارائه روش‌های تشخیص و مقابله با باتنت‌ها لازم است ضمن شناخت ساختار و فرایند حیات باتنت، رفتار ترافیکی و در واقع جریان‌های باتنتی به‌صورت دقیق مورد مطالعه قرار گیرد. با توجه به رسالت پدافند غیرعامل در خصوص تأمین امنیت و حصول اطمینان از عدم دسترسی‌های غیرمجاز به اطلاعات، ایمن‌سازی و اطمینان از پایداری و خلل‌ناپذیری در فعالیت شبکه‌های ارتباطی و در نهایت صحت و تداوم کارکرد صحیح شبکه و سامانه‌های الکترونیکی تحت شبکه گسترده اینترنت که منجر به توسعه ظرفیت دفاع الکترونیکی و تقویت ضریب امنیت و پایداری در حوزه زیرساخت‌های فناوری اطلاعات و ارتباطات می‌گردد و همچنین علم بر این موضوع که لازمه یک دفاع موفق در حملات سایبری بالا بردن سطح امنیتی عناصر درگیر است و این مهم جز با افزایش دانش در حوزه فضای مجازی میسر نخواهد بود، تحقیق حاضر در راستای تحقق اهداف پدافند غیرعامل سایبری و افزایش دانش شناسایی خصیصه‌ها و پایش یکی از بسترهای اصلی حملات اینترنتی می‌باشد.

در این مقاله در ادامه در بخش دو در مورد ساختار باتنت بحث خواهد شد. چرخه حیات باتنت‌ها موضوعی است که در بخش سوم مطرح می‌شود. بخش چهارم در مورد معماری باتنت‌ها مواردی را مطرح می‌کند و در بخش پنجم پروتکل‌های ارتباطی باتنت‌ها معرفی و توضیح داده می‌شوند و پس از آن در بخش ششم مشخصه‌هایی از ترافیک و جریان باتنتی متمرکز که توسط سامانه ارائه‌شده، مستند شده‌اند برای شناسایی آن از ترافیک و جریان عادی معرفی خواهد شد و در بخش آخر نتایج مقاله بررسی خواهد شد.

## ۲- ساختار باتنت

همواره اشکال متفاوتی از اقدامات در برخورد با فعالیت‌های مجرمانه در یک فضای سایبر وجود دارد، فارغ از این موضوع و بر مبنای اصول پدافند غیرعامل و فناوری اطلاعات، گام اول در یک دفاع سایبری شناسایی ساختمان و مراحل یک حمله است، بنابراین ابتدا باید درک صحیحی از چگونگی استقرار، ارتباط اجزا و مراحل مختلف در یک حمله مبتنی بر باتنت کسب و بر مبنای آن اقدامات امنیتی صورت گیرد. ساختار باتنت از سه قسمت عمده تشکیل شده است: بات، مدیر بات[5]، کانال فرمان و کنترل.

کلمه بات از تلخیص ربات به‌دست آمده است که در برخی منابع به آن زامبی[6] نیز گفته می‌شود. در واقع نوع جدیدی از بدافزارها[7] است که بر روی کامپیوترهای آسیب‌پذیر از راه‌های مختلف و بهره‌گیری از مکانیزم‌های انتشار منتقل‌شده و امکان کنترل توسط نفوذگر که به آن مدیر بات می‌گویند را برای اجرای دستورات خاصی (معمولا خرابکارانه) فراهم می‌آورد. پس از این‌که کد مورد نظر بر روی کامپیوتر نصب شد کامپیوتر اشغال‌شده تبدیل به یک بات یا زامبی می‌شود. برخلاف سایر انواع بدافزارها مانند ویروس یا کرم[8] که فعالیت اصلی آنها تمرکز بر روی میزبانی است که به آن نفوذ کرده اند، بات‌ها می‌توانند دستورات را از مدیر بات دریافت کرده و برای حمله به قربانی[9] اصلی مورد استفاده قرار گیرند [۳]. به اداره‌کننده بات و به عبارتی شخص یا گروهی از اشخاص که مدیریت و کنترل بات‌ها را از راه دور انجام می‌دهند، مدیر بات گفته می‌شود [۳]. یکی از تفاوت‌های میان باتنت و ویروس در امکان کنترل آنها است [۴]. باتنت از یک کانال فرمان و کنترل برای کنترل خود بهره می‌برد که بخش ضروری و اصلی شبکه بات همین ساختار فرمان و کنترل است و به اختصار به آن C&C گفته می‌شود. این زیرساخت شامل بات‌ها و

1- Botnet
2- Platform
3- Spam
4- Malicious code

5- Botmaster
6- Zombie
7- Badware
8- Worm
9- Victim

یک یا چند موجودیت کنترل است که بسته به ساختار بات‌نت می‌تواند عمل کنترل را به‌صورت متمرکز یا توزیعی انجام دهد. زیرساخت C & C به طور معمول به عنوان تنها راه برای کنترل بات‌ها در بات‌نت عمل می‌کند. بات‌ها در این زیرساخت برای اجرای موثر و مناسب دستورات نیاز به ارتباطی پایدار دارند [۲].

## ۳- چرخه حیات بات‌نت

### ۳-۱- انتشار[1]

بات‌نت می‌تواند در وسعت و ساختارهای مختلفی ایجاد شود اما همه آنها مراحل یکسانی را در چرخه حیات خود سپری می‌کنند. چرخه حیات بات‌نت پس از تولید کد دودویی مخرب با پروسه آلوده‌سازی سامانه‌های آسیب‌پذیر توسط انتشار فایل آلوده آغاز می‌شود. مدیر بات روش‌ها و تکنیک‌های مختلفی برای انتشار کد خود از طریق مکانیزم‌های انتشار در اختیار دارد. از جمله این تکنیک‌ها می‌توان به نامه های الکترونیکی آلوده، بهره‌گیری از نرم-افزارها و کرک‌ها اشاره کرد. پس از انتقال فایل دودویی به سامانه‌های آسیب‌پذیر و اجرای آنها، سامانه تبدیل به بات می‌شود [۵].

### ۳-۲- ارتباطات[2]

تفاوت عمده میان بات‌نت و سایر انواع بدافزارها وجود ارتباطات و بهره‌گیری از ساختار فرمان کنترل (C&C) است. C&C اجازه دریافت فرامین و دستورات از مدیر بات را برای بات فراهم می‌کند [۳]. به عبارت دیگر در مرحله ارتباطات، بات از طریق کانال در نظرگرفته شده برای فرمان و کنترل اقدام به برقراری ارتباط دوره‌ای با سرویس‌دهنده‌های فرمان و کنترل می‌کند. در این ارتباطات دستورات مورد نظر مدیر بات به بات منتقل می‌شود. به محض دریافت و شناسایی دستور جدید توسط بات، دستور دریافتی اجرا شده و نتایج اجرای آن به سرویس‌دهنده فرمان و کنترل گزارش می‌شود و سپس بات منتظر دریافت دستورات جدید باقی می‌ماند. البته کانال ارتباطی صرفا برای برقرای ارتباط میان بات و مدیر بات به منظور دریافت فرامین نیست، ارتباطات می‌توانند برای اعلام زنده بودن بات یا دریافت نسخه‌های جدید به سرویس دهنده‌های فرمان کنترل و یا حتی بین بات‌های یک بات‌نت برقرار شود. در هرصورت مدیر بات باید اطمینان حاصل کند که ساختار C&C برای مدیریت هزاران بات توزیع شده در سطح اینترنت به اندازه کافی قوی بوده و در مقابل تلاش‌هایی که برای شناسایی و ممانعت از برقراری ارتباطات صورت می‌گیرد عملکرد خوبی دارد.

### ۳-۳- حمله[3]

هدف اصلی و نهایی یک بات‌نت اجرای یک حمله است. بات‌ها براساس فرامین دریافتی اقدام به حمله به هدف مشخص شده توسط مدیر بات می‌کنند. ویژگی اصلی حملات مبتنی بر بات‌نت تعداد زیاد حمله‌کنندگان و عملکرد گروهی و هماهنگ آنها در یک شبکه بات است. برخی اوقات پس از انجام یک حمله بات‌ها اقدام به برقرای ارتباط با سرویس‌دهنده‌های خاصی کرده و پس از بروزرسانی برای حملات دیگری سازماندهی می‌شوند [۱]. بات‌نت‌ها عمدتا برای اجرای اقدامات خرابکارانه بر روی شبکه‌های کامپیوتری ایجاد می‌شوند [۵] درواقع بات‌نت یک حمله نیست بلکه ساختاری برای اجرای انواع مختلف و در عین حال خطرناک حملات بر روی شبکه‌های کامپیوتری و اینترنت است [۶]. تعیین آثار، نشانه‌ها و هشدارها بدین معنی که وقتی حمله‌ای اتفاق می‌افتد، باید آثار و خطراتی که این حمله می‌تواند داشته باشد را شناسایی کنیم، با شناسایی آثار یک حمله می‌توان از پیامدهای حملات دیگر و خطراتی که ممکن است ایجاد شوند، جلوگیری کرد به همین منظور در ادامه با برخی از حملات که با استفاده از بستر بات‌نت اجرا می‌شوند آشنا می‌شویم:

#### ۳-۳-۱- حملات انکار سرویس

نوعی از حملات هستند که در آن از ارائه یک سرویس جلوگیری به‌عمل آمده و آن را از دسترس خارج می‌کند. حملات انکار سرویس توزیع شده نوع خاصی از حملات انکار سرویس هستند که در آن چندین عامل حمله‌کننده به‌طور همزمان و هماهنگ و با هدف از کار انداختن و از دسترس خارج نمودن سرویس اقدام به حمله می‌کنند بنابراین ساختار بات‌نت‌ها برای ترتیب‌دادن این نوع از حملات کاملا مناسب است [۱]. با توجه به کنترل بات‌ها، مدیر بات می‌تواند با ارسال یک دستور خاص به بات‌ها، اجرای آن دستور و حمله DOS را از هزاران نقطه مختلف در سراسر اینترنت از بات‌ها بخواهند [۸-۷].

#### ۳-۳-۲- هرزنگاری[4]

به پیام‌های ناخواسته‌ای که در حجم بسیار زیادی از طریق رسانه‌های مختلفی مانند رایانامه، نرم‌افزارهای گفتگوی نوشتاری، ارسال نظر در وبلاگ‌ها یا وب‌سایت‌ها و گروه‌های خبری ارسال می‌شوند گفته می‌شود [۹]. براساس گزارش Kaspersky هشتادوپنج درصد از فعالیت‌های هرزنگاری توسط بات‌نت صورت می‌گیرد [۱۰] بنابراین ساختار بات‌نت می‌تواند به عنوان بستر اصلی جمع‌آوری و ساماندهی آدرس‌های نامه های الکترونیکی از کامپیوترهای به اشغال درآمده توسط بات‌نت و ارسال هرزنامه مورد استفاده قرار گیرد.

1- Spreading
2- Communications
3- Attack
4- Spam

براساس بررسی‌های به‌عمل آمده، هر بات به‌طور میانگین می‌تواند در هر ثانیه ۳ رایانامه یا پیام جعلی یا هرزنامه ارسال کند [۱۱].

### ۳-۳-۳-سرقت هویت

باتنت‌ها همچنین برای سرقت هویت[1] و اطلاعات استفاده از آنها در جهت منافع مدیران بات مورد استفاده قرار می‌گیرند. بات‌ها می‌توانند به‌گونه‌ای برنامه‌ریزی شوند که اطلاعات مهم و مشخص موجود در وب‌سایت‌ها را مورد کاوش قرار دهند [۶]. علاوه بر آن نرم‌افزارهای دیگری مانند گزارش‌گر کلیدها[2] توسط بات‌ها برای ثبت و گزارش اطلاعات مهمی مانند کلمات عبور و یا اطلاعات تجاری مانند خدمات بانکی برخط به مدیران بات منتشر می‌شوند [۱۲-۱۱].

### ۳-۳-۴- خدمات میزبانی، فروش و اجاره غیرقانونی

یک کامپیوتر یا سرور با فضای ذخیره‌سازی و اتصال با پهنای باند بالا بر روی اینترنت می‌تواند به عنوان یک هدف برای مدیر بات قرار گیرد تا با به‌دست گرفتن کنترل آن و استفاده برای خدماتی نظیر اشتراک فایل و میزبانی البته به‌صورت غیرقانونی مورد استفاده قرار دهد [۱۱]. برنامه‌های باتنت و سرویس‌های میزبانی برای فروش و یا اجاره برای دوره‌های معین موردنیاز جهت اهداف و مقاصد مجرمانه همواره در دسترس است. دلیل تمایل به این سرویس‌ها وجود موانع و فاصله بیشتر مابین خریداران و اجرای قانون است به عبارت بهتر امکان شناسایی حمله‌کننده اصلی که از این ساختار بهره می‌برد وجود ندارد [۱۳-۹].

### ۳-۳-۵- تبلیغ افزارها[3]

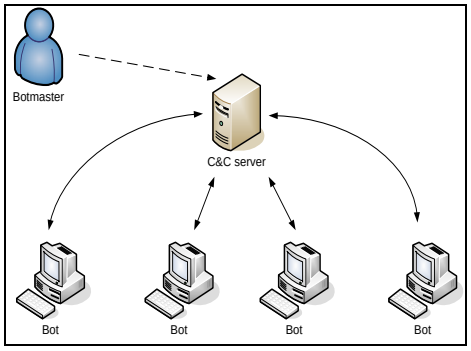
یکی دیگر از تفاوت‌های باتنت با سایر حملات و خطرات اینترنتی این است که باتنت‌ها می‌توانند برای صاحبان خود درآمد نیز تولید کنند. مدیران باتنت با استفاده از بات‌ها و بهره‌گیری از مزایای مالی بازدید از وب‌سایت‌هایی که این سرویس‌ها را ارائه می‌کنند درآمد هنگفتی عاید خود نمایند. ابزارهای تبلیغاتی نیز می‌توانند بر روی بات‌ها نصب شده و کاربران را مجبور به بازدید از صفحات خاصی از وب‌سایت‌ها کنند [۹]. علاوه بر حملات مورد بحث، باتنت‌ها می‌توانند برای گسترش انواع مختلف از تهدیدها در قالب ویروس‌ها، تروجان‌ها، درب پشتی، کرم‌ها و ... مورد استفاده قرار گیرند [۱۱].

## ۴- معماری باتنت‌ها

مکانیزم فرمان-کنترل برای انتقال داده‌ها مابین بات‌ها، سرویس‌دهنده‌های C&C و مدیر بات از معماری‌های مختلفی استفاده می‌کند بر این مبنا باتنت‌ها دارای سه معماری عمده هستند: مدل متمرکز، غیرمتمرکز و ترکیبی.

### ۴-۱- معماری متمرکز[4]

در معماری متمرکز فرمان و کنترل، یک یا چند سرویس‌دهنده وظیفه مدیریت ارتباطات را برعهده دارند در واقع مشخصه اصلی این معماری وجود یک یا چند نقطه مرکزی برای مدیریت ارتباطات است. مدیر بات یک میزبان را را برای ارسال فرمان‌ها و کنترل بات‌ها در نظر می‌گیرد. این میزبان می‌تواند یکی از کامپیوترهای آسیب‌پذیر و اشغال‌شده توسط مدیر بات باشد و یا یک سرویس‌دهنده قانونی که خدمات مربوط به سرویس‌دهی اینترنتی را انجام می‌دهد. زمانی که بات به کد دودویی آلوده شد اقدام به برقراری ارتباط با سرویس‌دهنده کرده و منتظر دریافت فرامین و تنظیمات موردنظر مدیر بات می‌ماند [۱۴]. در شکل۱معماری ساختار متمرکز فرمان و کنترل نشان داده شده است. مزیت این معماری امکان پیاده‌سازی سریع و مدیریت آسان بات‌ها و باتنت نقطه ضعف عمده آن این است که با حذف سرویس‌دهنده فرمان و کنترل کل باتنت از بین خواهد رفت [۱۱].




**شکل ۱- معماری ساختار متمرکز فرمان-کنترل [۱۴]**

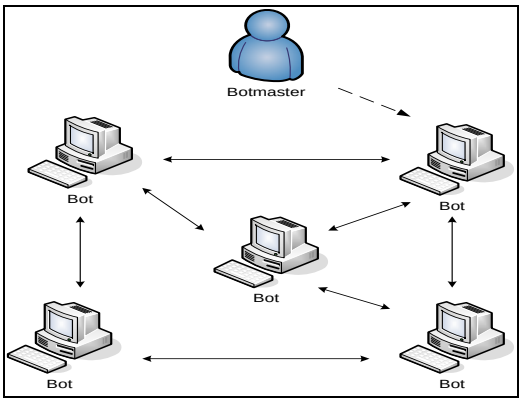
### ۴-۲- معماری غیرمتمرکز[5]

در معماری غیرمتمرکز فرمان-کنترل مدیر بات فرامین و تنظیمات را از چند نقطه بصورت غیرمتمرکز به بات‌ها ارسال می‌کند. ارتباطات بات‌ها و اعلام زنده بودن آنها نیز از طریق یک سرویس-دهنده صورت نمی‌گیرد. بات‌ها تحت یک توپولوژی تصادفی و غیرمتمرکز فرمان و کنترل اقدام به برقراری ارتباطات خود می‌کنند. در این معماری هر بات می‌تواند به عنوان سرویس‌دهنده فرمان و کنترل نیز عمل کند بنابراین دستورات از طریق یک بات به بات دیگر نیز منتقل می‌شود در این دستورات معمولا به بات گفته می‌شود که

1- Identity theft
2- Keylogger
3- Adware

4- Centralized
5- Decentralized

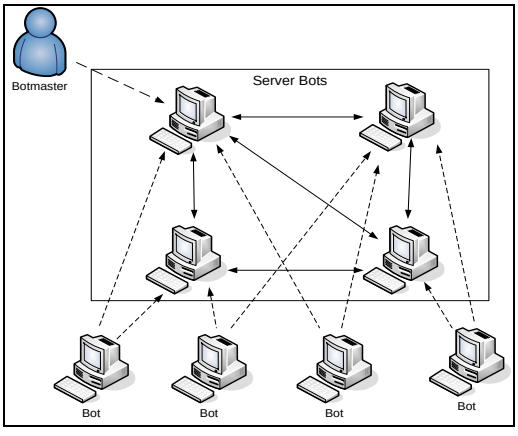
دستورات را میان عامل‌های دیگر گسترش دهد [۳]. پیاده‌سازی این ساختار و مدیریت آن پیچیده‌تر از مدل متمرکز است اما مشکل نقطه یگانه شکست توپولوژی متمرکز در این روش حل شده است و با شناسایی و حذف یک سرویس‌دهنده فرمان و کنترل، کل بات‌نت از بین نمی‌رود [۱۴]. شکل۲ معماری غیرمتمرکز فرمان و کنترل را نمایش می‌دهد.




**شکل ۲- معماری غیرمتمرکز فرمان و کنترل [۱۴]**

## ۴-۳- مدل ترکیبی[1]

همان‌گونه که شرح داده شد هر یک از معماری‌های متمرکز و غیرمتمرکز فرمان و کنترل با توجه به ساختار خود، مزایا و معایبی را به همراه داشتند. هدف از ایجاد معماری ترکیبی فرمان و کنترل بهره‌گیری از مزایا و کاهش دادن نقاط ضعف دو توپولوژی قبلی بصورت همزمان بوده است [۱۴]. این رویکرد ترکیبی از دو ساختار متمرکز و غیرمتمرکز است. معماری ترکیبی فرمان و کنترل در شکل ۳ نمایش داده شده است.




**شکل ۳- معماری ترکیبی فرمان و کنترل [۱۴]**

1- Hybrid

## ۵-پروتکل‌های[2] ارتباطی بات‌نت

بات‌نت‌ها معمولا از پروتکل‌های ارتباطی شناخته شده برای ارتباطات خود استفاده می‌کنند. در [۱۵]. پروتکل‌های ارتباطی بات‌نت‌ها در سه گروه مختلف معرفی دسته‌بندی شده‌اند.

### ۵-۱- پروتکل IPX[3]

یکی از رایج‌ترین پروتکل‌ها برای ارتباط با بات‌ها که توسط مدیر بات مورد استفاده قرار می‌گیرد پروتکل IRC است. پروتکل IRC عموما برای ارتباطات یک به چند طراحی شده است اما می‌توان از آن برای ارتباطات یک به یک که برای کنترل بات‌نت بسیار مناسب است، نیز بهره برد. پیکربندی ابزارها و سامانه‌های امنیتی برای بلوکه کردن ترافیک مربوط به پروتکل IRC به سادگی صورت می‌گیرد.

### ۵-۲- پروتکل HTTП[4]

یکی دیگر از پروتکل‌های مورد استفاده بات‌نت‌ها که از محبوبیت زیادی نیز برخوردار است پروتکل HTTP است. بات‌نت‌هایی که از پروتکل HTTP استفاده می‌کنند به سختی قابل شناسایی هستند. بات‌نت‌ها از طریق این پروتکل قادر به دور زدن سامانه‌های تأمین امنیت شبکه هستند. امتیاز و ویژگی استفاده از این پروتکل این است که ترافیک بات‌نتی در میان ترافیک معمول و عادی وب مخفی می‌شود و امکان فریب فایروال‌ها و مکانیزم‌های کنترل پورت IDSها را فراهم می‌آورد.

### ۵-۳- پروتکل П2П[5]

اخیرا بات‌نت‌های پیشرفته و هوشمند از پروتکل دیگری به نام P2P در ارتباطات خود بهره می‌برند [۱۶].

## ۶- پایش مشخصه‌های جریان‌های بات‌نتی با ارائه یک سامانه آنالیزترافیک

قرارگیری در یک حمله واقعی و تجربه شرایط و ویژگی‌های مختلف یک حمله بحثی است که در دانش پدافند غیرعامل تحت عنوان مانور از آن نام برده می شود بر همین مبنا ضمن پیاده‌سازی یک شبکه آلوده به بات‌نت و استقرار یک سامانه نرم‌افزاری پایشگر ترافیک شبکه به بررسی مشخصات جریان‌های بات‌نتی پرداخته و نتایج مشاهدات حاصل از آن مستند شده است.

2-Protocol
3- Internet Relay Chat
4 -Hypertext Transfer Protocol
5 -Peer to Peer

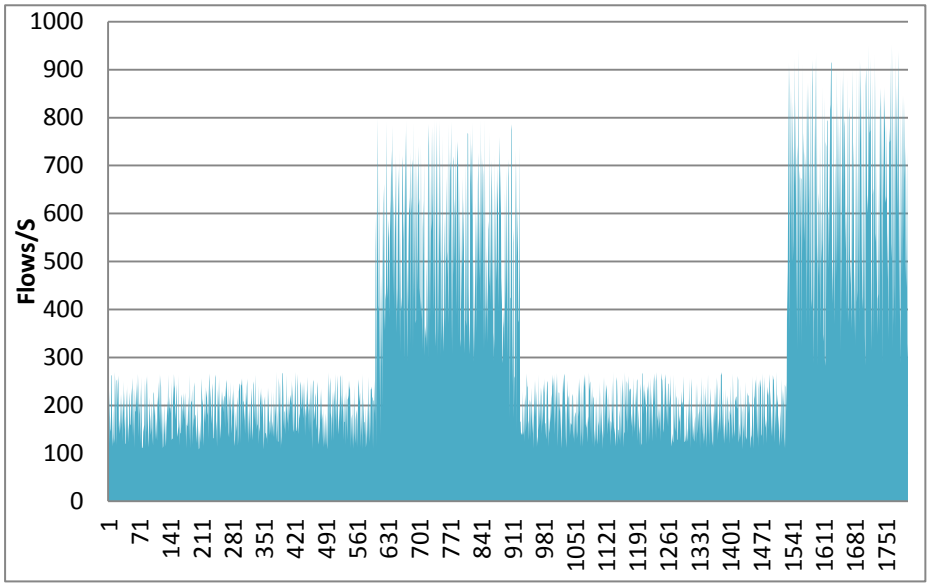
### ۶-۱- محیط پیاده‌سازی

برای پیاده‌سازی سامانه تحلیل ترافیک شبکه و پایش رفتار و جریان بات‌نتی، در طول انجام تحقیق با چالش‌های مختلفی روبرو بودیم که اصلی‌ترین آنها ایجاد و راه‌اندازی زیرساخت لازم و به‌خصوص سامانه ایجاد شبکه بات به نحوی که ارتباطات و ترافیک واقعی بات‌نت را ایجاد نماید بود. ساختار سناریو مورد نظر در یک شبکه با ۳۰ کامپیوتر که ۱۲ کامپیوتر در آن به عنوان بات، یک سرویس‌دهنده فرمان و کنترل خارج از شبکه مذکور و یک مدیر بات که از طریق سامانه‌های دیگر امکان دسترسی تحت وب جهت مدیریت و کنترل بات‌ها را در اختیار داشت پیاده‌سازی گردیدبرای ایجاد شبکه بات و تولید ترافیک بات‌نتی بر روی یکی از سامانه‌ها، اقدام به پیکربندی و راه اندازی یک سرویس‌دهنده وب، تحت سرویس‌دهنده وب Apache نموده‌ایم و سپس یک بات‌سرور متمرکز بر روی آن راه‌اندازی کردیم. یکی از قویترین بات‌نت‌ها به نام Zeus بر روی این سرویس‌دهنده راه‌اندازی گردید. تنظیمات مربوط به Zeus صورت گرفت و فایل config مربوط به تنظیمات آدرس بات‌سرور و زمان‌های برقراری ارتباط و همچنین یک فایل آلوده‌کننده برای آلوده‌سازی سامانه‌های آسیب‌پذیر تولید شد. فایل آلوده‌کننده به روی این سرویس‌دهنده راه‌اندازی گردید. تنظیمات مربوط به Zeus صورت گرفت و فایل config مربوط به تنظیمات آدرس بات‌سرور و زمان‌های برقراری ارتباط و همچنین یک فایل آلوده‌کننده برای آلوده‌سازی سامانه‌های آسیب‌پذیر تولید شد. فایل آلوده‌کننده به سامانه‌های معینی که نقش بات را در سناریوهای ما بازی می‌کردند منتقل و اجرا شدند.تمام جریان‌های شبکه از طریق سرویس‌دهنده ISA[1] به مقصد هدایت شده‌اند و در واقع برای مدیریت جریان‌های شبکه از یک سرویس‌دهنده ISA به همراه بانک اطلاعاتی SQLServer و زبان برنامه‌نویسی PHP و همچنین سرویس‌دهنده Apache بهره برده‌ایم. اطلاعات ترافیک شبکه از طریق سرویس‌دهنده ISA به بانک اطلاعاتی SQL هدایت و در جداولی برای تحلیل ذخیره شده‌اند. ابزار پایشگر شبکه Wireshark نیز جهت مشاهده اطلاعات جریان‌ها مورد استفاده قرار گرفته است.

### ۶-۲- بررسی مشاهدات رفتار بات‌نت‌ها

#### ۶-۲-۱- افزایش ترافیک شبکه[2]

با توجه به پایش وضعیت ترافیک شبکه در طول آزمایشات و دقت در رفتار ترافیکی بات‌نت‌ها در مرحله کنترل و فرمان مشاهده گردید که بات‌ها در این مرحله اقدام به برقراری ارتباطات پی‌درپی با بات‌سرور می‌نمایند این ارتباطات جهت اعلام زنده بودن و همچنین دریافت تنظیمات و دستورات مورد نظر مدیر بات‌نت می‌باشد. بنابراین مشخصه‌ی اول ناهنجاری بات‌نتی مربوط به تعداد ارتباطات بوده و مشخصا حجم ارتباطات زیاد در یک دوره زمانی نسبت به بقیه ارتباطات می‌باشد. به عبارت بهتر سامانه‌های آلوده یا بات‌ها تعداد بیشتری از ارتباطات پی‌درپی را با یک آدرس خاص به عنوان بات‌سرور برقرار نمودند. این ارتباطات حجم ترافیک شبکه را بالا می‌برد [۱۸-۱۷]. شکل ۴ افزایش میزان ترافیک شبکه را در طول مدت برقراری ارتباطات نشان می‌دهد.

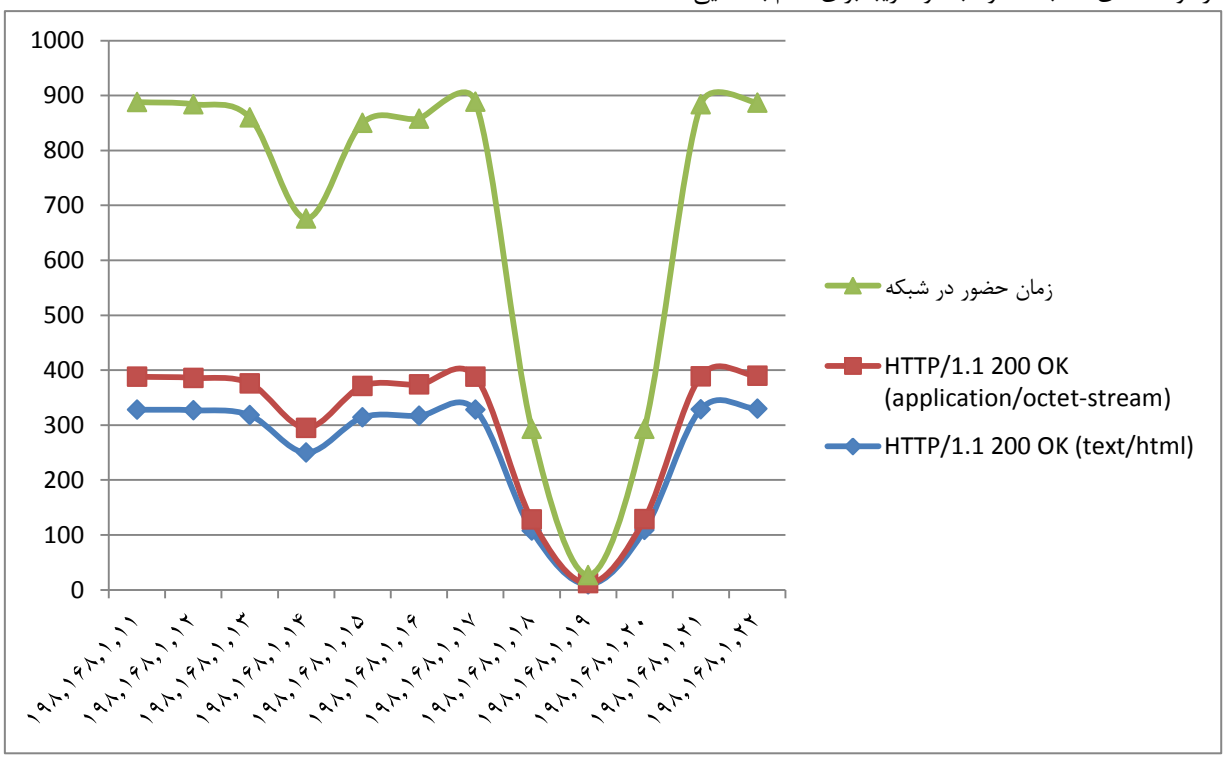



**شکل ۴- افزایش ترافیک شبکه در طول دوره‌های فرمان و کنترل**

1 -Internet Security and Acceleration Server
2 -Network traffic

### ۶-۲-۲- رفتار و درخواست‌های مشابه[1] بات‌ها

بات‌های عضو یک گروه به دلیل تنظیمات و اجرای دستورات یکسان معمولا درخواست‌ها و رفتارهای مشابهی در شبکه از خود نشان می‌دهند [۱۹]. با توجه به تحلیل نتایج صورت گرفته توسط سامانه پایشگر و تحلیل ترافیک مشاهده شد با توجه به عضویت بات‌ها در یک گروه، درخواست‌های مشابهی از سوی آنها ارسال می‌شود. آمار این درخواست‌های مشابه معمولا بالا و تقریبا برای تمام بات‌هایی که مدت زمان مشابهی در شبکه حضور داشته‌اند یکسان است. شکل ۵ این موضوع را به خوبی نشان داده است. بات‌ها با آدرس ۱۱ و۱۲و ۱۳و ۱۵و ۱۶ و ۱۷ و ۲۱و ۲۲ با توجه به این‌که مدت زمان یکسانی در شبکه حضور داشته‌اند تقریبا دارای تعداد یکسانی از درخواست های مشابه ارسالی به سرویس‌دهنده فرمان و کنترل هستند.

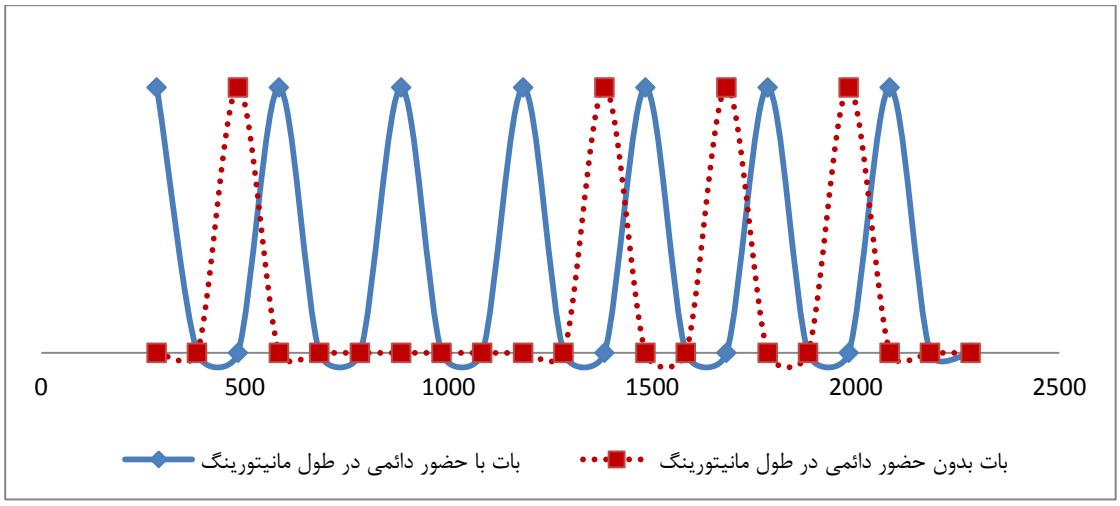



**شکل ۵- میزان درخواست‌های ارسالی سامانه‌های آلوده به سرویس‌دهنده فرمان و کنترل**

### ۶-۲-۳- ارتباطات دوره‌ای[2] بات با سرویس‌دهنده فرمان و کنترل

با توجه به برنامه‌های از پیش تعیین شده برای بات‌ها، آنها در دوره‌های زمانی منظمی با سرویس‌دهنده فرمان و کنترل ارتباط برقرار کرده و ضمن اعلام زنده بودن، تنظیمات و فرامین مدیر بات را دریافت می‌کنند. نتیجه این ارتباطات یک رفتار منظم و دوره‌ای میان سرویس‌دهنده C&C و بات می‌باشد. در انواع مختلف شبکه‌های بات در دوره‌های زمانی منظمی این ارتباطات برقرار می‌شود [۲۰]. البته ممکن است به دلایل مختلفی مانند خاموش بودن سامانه یا قطع بودن ارتباط شبکه بات و به طور کلی عدم حضور بات در شبکه این رفتار دوره‌ای کامل نشود. شکل ۶ درخواست‌های یکسان دو بات در یک دوره زمانی را نمایش می‌دهد. نقاط مشخص شده در رأس سهمی‌هایی که با خط ممتد رسم شده اند زمان‌های برقراری ارتباط توسط سیستم کامپیوتری آلوده‌ای را نمایش می‌دهند که در کل دوره پایش در شبکه حضور داشته است. با اتصال این نقاط به یکدیگر یک نمودار هارمونیک و منظم بوجود می‌آید این نمودار موید برقراری ارتباطات در فواصل زمانی منظم میان بات و سرویس‌دهنده فرمان- کنترل است. نقاط مشخص شده در رأس سهمی‌های رسم شده با خط‌چین موجود در شکل ۶ نیز مربوط به زمان‌های ارتباط باتی است که عمدا ارتباط آن با شبکه قطع شده است. با اتصال این نقاط به یکدیگر عدم وجود هارمونی در زمان‌های ارتباط این بات کاملا مشهود شده است.

1-Similar requests
2- Periodically communications




**شکل۶- نمودار Time Stamp برقراری ارتباط بات با سرویس‌دهنده C&C**

**۶-۲-۴- زمان پاسخگویی[1] کوتاه و اجرای سریع فرامین** باتها معمولا بلافاصله پس از دریافت دستورات مدیر بات به آن پاسخ می‌دهد. این زمان پاسخگویی نسبت به زمان پاسخگویی بشر بسیار کمتر است. علاوه بر زمان پاسخگویی کوتاه ، بات دستورات مشخص مدیر بات را بلافاصله اجرا می‌کند [۲۱]. سامانه ارائه شده با بررسی عکس العمل باتها پس از دریافت فرامین از مدیر بات زمان پاسخگویی و اجرای فرامین توسط بات را به طور متوسط کمتر از 1ms ارزیابی کرده است.

**۶-۲-۵- اندازه کوچک دستورات[2]**

طول بسته‌ها در ترافیک معمول وب در حالت عادی نسبتا بزرگ است. به منظور جلوگیری از افزایش بار سرویس‌دهنده باتنت‌ها تمایل به دستورات با حجم بسته‌ای کوچک دارند [۱۷]. طول بسته‌ها و دستورات مدیر بات که جهت اجرا به بات ارسال می‌شود معمولا 1KB و حتی کمتر از آن است [۲۲]. با بررسی دستورات ارسالی به باتها این موضوع کاملا مشخص و آشکار گردید.

**۶-۲-۶- مخفی ماندن ترافیک باتنت**

با توجه به اینکه باتنت از پروتکل‌های استاندارد شبکه برای ارتباطات خود استفاده می‌کنند فعالیت آنها در میان ترافیک هنجار و طبیعی وب مخفی مانده و توسط سامانه‌های امنیتی و فایروال‌ها مورد شناسایی قرار نمی‌گیرند. با توجه به این‌که پروتکل HTTP برخلاف پروتکل‌های IRC و P2P برای ارائه گستره وسیعی از خدمات و سرویس‌های اینترنتی مورد استفاده قرار گرفته است نمی‌توان به راحتی این پروتکل و سرویس‌های آن را کنار گذاشت [۱۱]. در شبکه مورد آزمایش نیز مخفی ماندن ترافیک باتنتی در میان ترافیک عادی موجبات عدم شناسایی توسط سامانه‌های امنیتی را باعث گردید.

## ۷- نتیجه‌گیری

باتنت به عنوان یکی از فراگیرترین و مخربترین حملات در اینترنت، یکی از جذاب‌ترین زمینه‌های فعالیت و تحقیق برای پژوهشگران امنیت شبکه به حساب می‌آید. شناخت و درک ساختار، نحوه عمل و ویژگی‌های مختلف باتنت منجر به تعریف استراتژی‌ها و راه حل‌های کشف و مقابله با باتنت خواهد شد. در این مقاله با پیاده‌سازی یک شبکه آلوده به بات و ارائه سامانه پایشگر ترافیک شبکه تحلیلی از باتنت‌ها و جریان باتنتی توسط پایش جریان با دو هدف ارائه شد: ۱- شناسایی ساختار و چرخه حیات باتنت، انواع باتنت از نظر توپولوژی و پروتکل مورد استفاده، ۲- تمرکز بر روی جریان‌های باتنتی و رفتار باتنت و برجسته کردن ویژگی‌های آن جهت بهره‌گیری در الگوریتم‌های تشخیص و مقابله با باتنت. از دید پدافندی می‌توان گفت با شناسایی مشخصه‌های جریان و ترافیک مربوط به مرحله فرمان و کنترل باتنت و ارائه ساختارهای تحلیل و بررسی ترافیک شبکه و فیلتر بر مبنای ویژگی‌های مذکور می‌توان تا حد چشمگیری از تشکیل شبکه‌های گسترده بات در اینترنت جلوگیری بعمل آورد. با توجه به اینکه باتنت‌ها بستر اصلیِ بخش عمده‌ای از حملات در اینترنت هستند و ماهیت حملات مبتنی بر باتنت به گونه‌ای است که پس از وقوع فاز نهایی حمله امکان مقابله

1 -Response time
2-Little command size

و کاهش آسیب‌ها به حداقل می‌رسد، بنابراین تحقیق بر روی شاخصه‌های ترافیک بات‌نتی و طراحی و ارائه الگوریتم و معماری‌های آنالیز و تشخیص ترافیک بر مبنای رفتار ترافیکی و تشخیص ناهنجاری در مرحله کنترل و فرمان به عنوان راهکاری موثر برای مقابله با حملات مبتنی بر بات نت پیشنهاد مطالعات آتی این مقاله است.

## ۸- مراجع


1. R. A. Rodríguez-Gómez, "G. Maciá-Fernández and P. García-Teodoro, Analysis of botnets through life-cycle," Security and Cryptography (SECRYPT), 2011 Proceedings of the International Conference on, Seville, Spain, pp. 257-262, 2011.
2. C. Elliott, "Botnets: To What Extent Are They a Threat to Information Security?," Information Security Technical Report, vol. 15, pp. 79-103, 2010.
3. H. R. Zeidanloo and A. A. Manaf, "Botnet Command and Control Mechanisms," Computer and Electrical Engineering, 2009 ICCEE '09, Second International Conference on, Dubai, pp. 564-568, 2009.
4. T. Cai and F. Zou, "Detecting HTTP Botnet with Clustering Network Traffic," Wireless Communications, Networking and Mobile Computing (WiCOM), 2012 8th International Conference on, Shanghai, China, pp. 1-7, 2012.
5. N. Hachem, Y. Ben Mustapha, G. G. Granadillo, and H. Debar, "Botnets: Lifecycle and Taxonomy," Network and Information Systems Security (SAR-SSI), 2011 Conference on, La Rochelle, pp. 1-8, 2011.
6. M. Chandramohan and H. B. K. Tan, "Detection of Mobile Malware in the Wild," in Computer, vol. 45, no. 9, pp. 65-71, Sept. 2012.
7. C. Li, W. Jiang, and X. Zou, "Botnet: Survey and Case Study," Innovative Computing, Information and Control (ICICIC), 2009 Fourth International Conference on, Kaohsiung, pp. 1184-1187, 2009.
8. E. Yuce, "A Literature Survey about Recent Botnet Trends," GÉANT Network, ULAKBIM, Turkey, Rep. JRA2 T4, 2012.
9. C. Elliott, "Botnets: To What Extent Are They a Threat to Information Security?," Information Security Technical Report, vol. 15, pp. 79-103, 2010.
10. V. Kamluk, "The Botnet Ecosystem [Online].Available: http://www.securelist.com/en/analysis/204792095/The_Botnet_ecosystem, 2009.
11. M. Eslahi, R. Salleh, and N. B. Anuar, "Bots and botnets: An overview of characteristics, detection and challenges," Control System, Computing and Engineering (ICCSCE), IEEE International Conference on, Penang, pp. 349-354, 2012.
12. B. Stone-Gross, M. Cova, B. Gilbert, R. Kemmerer, C. Kruegel, and G. Vigna, "Analysis of a Botnet Takeover," in IEEE Security & Privacy, vol. 9, no. 1, pp. 64-72, Jan.-Feb. 2011.
13. Cisco, "Cisco 2009 Midyear Security Report: An Update on Global Security Threats and Trends," Cisco Systems, Rep., 2009.
14. M. Bailey, E. Cooke, F. Jahanian, Y. Xu, and M. Karir, "A Survey of Botnet Technology and Defenses," Conference for Homeland Security, 2009 CATCH '09, Cyber security Applications & Technology, Washington, DC, pp. 299-304, 2009.
15. Taxonomy of Botnet Threats, "Trend Micro Inc.," White Paper, November 2006.
16. J. B. Grizzard, V. Sharma, C. Nunnery, B. B. Kang, and D. Dagon, "Peer-to-peer Botnets: Overview and case study," In Proc. of OT Topics in Understanding Botnets (HotBots'07), pp.198-201, 2007.
17. T. Cai and F. Zou, "Detecting HTTP Botnet with Clustering Network Traffic," Wireless Communications, Networking and Mobile Computing (WiCOM), 8th International Conference on, Shanghai, China, pp. 1-7, 2012.
18. C. M. Chen, Y. H. Ou, and Y. C. Tsai, "Web botnet detection based on flow information," Computer Symposium (ICS), International, Tainan, pp. 381-384, 2010.
19. S. Arshad, M. Abbaspour, M. Kharrazi, and H. Sanatkar, "An anomaly-based botnet detection approach for identifying stealthy botnets," Computer Applications and Industrial Electronics (ICCAIE), IEEE International Conference on, Penang, pp. 564-569, 2011.
20. B. Assadhan, J. M. F. Moura, and D. Lapsley, "Periodic Behavior in Botnet Command and Control Channels Traffic," Global Telecommunications Conference, GLOBECOM, IEEE, Honolulu, HI, pp. 1-6, 2009.
21. M. M. Masud, T. Al-khateeb, L. Khan, B. Thuraisingham, and K. W. Hamlen, "Flow-based identification of botnet traffic by mining multiple log files," Distributed Framework and Applications, DFM, First International Conference on, Penang, pp. 200-206, 2008.
22. T.-M. Koo, H.-C. Chang, and G.-Q. Wei, "Construction P2P firewall HTTP-Botnet defense mechanism," Computer Science and Automation Engineering (CSAE), IEEE International Conference on, Shanghai, pp. 33-39, 2011.

# Monitoring the Flow Characteristics of Botnet with a Network Traffic Analysis System

**M. Rahimipour, A. Firouzy, Sh. Jamali***

## Abstract

Botnet is one of the important but little-known dangers on the Internet. Botnets are networks of compromised computers that are controlled through a command-and-control channels for destructive attacks in the vast expanses. Botnets are often used for malicious activities such as distributed denial of service attacks. To deal with these type of attack is required to study and examine the structure, properties and behavior of botnet traffic. Therefore, identification of the main characteristics of botnets and monitoring the flows of botnet will be effective in creating and developing technologies to deal with this potential security risk. In this work, are reviewed botnets and their life cycle and types of topologies and protocols they use and documented the behaviors and characteristics of botnet traffic with implementation a network of botnet-infected And provide a network flow analysis system. Find these features to provide solutions to detect and deal with botnet-based attacks will be effective.

**Key Words:** *Botnet, Flow, Attack, Command-And-Control*

* University of Mohaghegh Ardebili (jamali@iust.ac.ir) - Writer-in-Charge