بسم الله الرحمن الرحيم

دانشگاه پیام نور استان تهران

مرکزتهران غرب

پایان نامه

برای دریافت مدرک کارشناسی ارشد

رشته مدیریت فناوری اطلاعات

عنوان پایان نامه :

ارائه روشی برای حفاظت سرویسهای وب از حملات باتنت با بکارگیری روش ترکیبی API Verifier و Enhanced Captcha

امیر حسن داودنژاد

استاد راهنما :

دکتر داود کریم زادگان مقدم

استاد مشاور :

داود وحدت

اردیبهشت ماه ۹۳

گواهی اصالت، نشر و حقوق مادی و معنوی اثر

اینجانب امیرحسن داودنژاد دانشجوی ورودی سال ۱۳۹۰ مقطع کارشناسی ارشد رشته مدیریت فناوری اطلاعات گواهی می‌نمایم چنانچه در پایان نامه خود از فکر، ایده و نوشته دیگری بهره گرفته‌ام با نقل قول مستقیم یا غیر مستقیم منبع و ماخذ آن را نیز در جای مناسب ذکر کرده‌ام. بدیهی است مسئولیت تمامی مطالبی که نقل قول دیگران نباشد بر عهده خویش می‌دانم و جوابگوی آن خواهم بود.

دانشجو تایید می‌نماید که مطالب مندرج در این پایان نامه (رساله) نتیجه تحقیقات خودش می‌باشد و در صورت استفاده از نتایج دیگران مرجع آن را ذکر نموده است.

نام و نام خانوادگی دانشجو: امیرحسن داودنژاد

تاریخ و امضاء:

اینجانب امیرحسن داودنژاد دانشجوی ورودی سال ۱۳۹۰ مقطع کارشناسی ارشد رشته مدیریت فناوری اطلاعات گواهی می‌نمایم چنانچه بر اساس مطالب پایان نامه خود اقدام به انتشار مقاله، کتاب و ... نمایم ضمن مطلع نمودن استاد راهنما، با نظر ایشان نسبت به نشر مقاله، کتاب، و... و به صورت مشترک و با ذکر نام استاد راهنما مبادرت نمایم.

نام و نام خانوادگی دانشجو: امیرحسن داودنژاد

تاریخ و امضاء:

کلیه حقوق مادی مترتب از نتایج مطالعات، آزمایشات و نوآوری ناشی از تحقیق موضوع این پایان نامه متعلق به دانشگاه پیام نور می باشد.

اردیبهشت ماه ۱۳۹۳

تقدیم به

آنان که زندگی خود را وقف آگاهی انسان‌ها می نمایند

همچنین به **خانواده عزیزم** که در تمامی سالهای تحصیلی‌ام مرا در نزدیک شدن به اهدافم یاری رساندند

امیرحسن داودنژاد

اردیبهشت ماه ۹۳

تشکر و قدردانی

سپاس بی‌کران پروردگار یکتا را که هستی‌مان بخشید و به طریق علم و دانش رهنمونمان شد

از استاد گرامی **جناب آقای دکتر داود کریم زادگان مقدم** به سبب قبول زحمت هدایت این تحقیق کمال تشکر را دارم.

از استاد گرامی **جناب آقای دکتر داود وحدت** به سبب راهنمایی‌های بسیار با ارزششان کمال سپاس و امتنان را دارم.بی شک بدون حمایت‌های بی دریغ شان انجام این تحقیق میسر نمی‌گردید.

امیرحسن داودنژاد

اردیبهشت ماه ۹۳

چکیده

باتنت‌ها به دلیل گستردگی حجم حملات و زیان‌های مالی فراوان بزرگترین تهدید جامعه سایبری محسوب می‌گردند. باگسترش روز افزون وب۲ و شبکه‌های اجتماعی طراحان باتنت‌ها از این شبکه‌های اجتماعی جهت برقراری ارتباط میان بات و بات‌مستر، ارسال اطلاعات و دریافت دستورات استفاده می‌نمایند.

بات‌های فعال در فضای سایبری جامعه آماری مورد استفاده دراین تحقیق بوده و با توجه به اینکه اولین گام در مقابله با باتنت‌ها شناسایی آنها است و طراحان باتنت از ابتدا به طراحی باتنت نمی‌پردازند، روش تحقیق بکارگرفته شده شناسایی باتنت‌ها در دو حوزه بر پایه میزبان و بر پایه شبکه می‌باشد. ابزارها و تکنیک‌های مورد استفاده دراین تحقیق آنالیزترافیک، هانی‌پات و شناسایی نقاط آسیب‌پذیر نرم‌افزارها می‌باشد.

سیستم پیشنهادی روش ترکیبی تصدیق‌کننده ای‌پی‌آی و کپچای بهبود یافته جهت جلوگیری از سوءاستفاده از سرویس‌های وب می‌باشد. تصدیق‌کننده ای‌پی‌آی از دو جز اصلی تشکیل گردیده است: تصدیق‌کننده ای‌پی‌آی کلاینت و تصدیق‌کننده ای‌پی‌آی سرور. سیستم کپچا بهبودیافته نیز از دو قسمت عمده تشکیل شده است: کلاینت و سرور.

وظیفه اصلی تصدیق‌کننده ای‌پی‌آی تشخیص فراخواننده ای‌پی‌آی جهت تمایز میان بات و کاربر عادی بوده و وظیفه اصلی کپچای بهبودیافته جلوگیری از انتشار باتنت‌ها می‌باشد.

با توجه به مطالعات بعمل آمده و شبیه‌سازی‌های انجام شده در این تحقیق سیستم پیشنهادی از انتشار باتنت‌ها و حملات صورت گرفته نظیر اسپوفینگ مک‌آدرس، کلاهبرداری از تصدیق‌کننده ای‌پی‌آی کلاینت و عبورکردن از تاییدکننده کپچا با فاصله اطمینان مناسب درشبکه‌های تست شده جلوگیری بعمل آورده و باعث حفاظت سرویس‌های وب می‌گردد. و این مدل بعنوان خروجی نهایی جهت استفاده ارائه گردید.

واژه‌های کلیدی: باتنت، امنیت، فضای سایبری، کپچای بهبود یافته، تصدیق‌کننده ای‌پی‌آی

فهرست مطالب

فهرست جداول

فهرست شکلها

فصل اول

کلیات تحقیق

مقدمه

امروزه باتنت‌ها[1] به دلیل گستردگی، حجم حملات، زیان های مالی فراوان، تاثیرات مخربی که بر پهنای باند شبکه‌های رایانه‌ای و قدرت پردازش وب سرورها دارند بزرگترین تهدید اینترنت و جامعه سایبری محسوب می‌گردند. حمله سایبری صورت گرفته به کشور استونی در سال ۲۰۰۷ بوسیله هکرهای روسی ازطریق باتنت‌ها از جمله بارزترین حملات سایبری در سطح جهانی می‌باشد. از آن زمان تاکنون به باتنت‌ها به عنوان یک ابزارمهم در جنگ‌های سایبری توجه ویژه‌ای می‌گردد ودر تمامی کشورها، توسط مدیران امنیت رایانه‌ای استراتژی‌ها و تدابیر ویژه‌ای جهت مبارزه با اینگونه حملات درنظر گرفته می‌شود.(ژوسک[2]،۲۰۱۲)

باتنت‌ها فعالیتهای تحت وب کاربران را بدون اطلاع یا رضایت کاربر کنترل کرده و گزارش می‌دهند. باتنت‌ها همچنین نرم‌افزارهای دیگری را برای جمع‌آوری اطلاعات درباره آسیب‌پذیریهای سیستم نصب کرده و این اطلاعات را به دیگران می‌فروشند. علاوبراین یک بات می‌تواند بعنوان یک وسیله استراق سمع بکاررفته و داده‌های مهم و حساس را که ازیک سیستم آسیب دیده می‌گذرند گوش دهد.

یک باتنت با هزاران عضوی که در سراسر جهان دارد می‌تواند یک حمله گسترده و هماهنگ را برای خراب کردن با از کار انداختن سایتها و سرویس‌های مهم راه اندازی نماید و منابع و پهنای باند این سیستمها را اشغال کند. هدف این حملات ممکن است شامل وب سایتهای تجاری یا دولتی، سرویس‌های ایمیل، زیرساخت‌های اینترنت یا حتی تولیدکنندگان ابزارهای امنیتی صنعت فناوری اطلاعات باشد. حملات همچنین ممکن است سازمانهای سیاسی و یا کشورهای خاصی را هدف بگیرند. باتنت‌ها فعالیتهای تحت وب کاربران را بدون اطلاع یا رضایت کاربر کنترل کرده و گزارش می‌دهند. همچنین ممکن است نرم‌افزار دیگری را برای جمع‌آوری اطلاعاتی درباره آسیب‌پذیریهای سیستم نصب کرده و این اطلاعات را به دیگران بفروشند. یک بات می‌تواند به عنوان یک وسیله استراق سمع به کار رفته و داده‌های مهم و حساس را که از یک سیستم آسیب دیده می‌گذرند گوش دهد. باگسترش روز افزون وب۲ و شبکه‌های اجتماعی از قبیل فیس‌بوک و تویتر

[1] Botnet
[2] Czosseck

طراحان باتنت‌ها از این شبکه‌های اجتماعی جهت برقراری ارتباط میان بات و بات‌مستر، ارسال اطلاعات ودریافت دستورات استفاده می‌نمایند. در این تحقیق پس از مطالعه رفتار و عملکرد باتنت‌ها به ارائه روشی جهت مقابله با سوءاستفاده از سرویس‌های وب با بکارگیری روش ترکیبی تصدیق‌کننده ای‌پی‌آی و کپچای بهبودیافته می‌پردازیم.

تصدیق‌کننده ای‌پی‌آی از دو جز اصلی تشکیل گردیده است: تصدیق‌کننده ای‌پی‌آی کلاینت و تصدیق‌کننده ای‌پی‌آی سرور. وظیفه اصلی تصدیق‌کننده ای‌پی‌آی تشخیص اینکه فراخواننده ای‌پی‌آی کاربر عادی است یا بات، می‌باشد. در صورتی که فراخواننده ای‌پی‌آی بات باشد از دسترسی به ای‌پی‌آی جلوگیری بعمل می‌آورد.

سیستم کپچا از دو قسمت عمده تشکیل شده است: کلاینت و سرور. قسمت سرور مسئول تولید کپچا و پردازش پاسخ تولید شده توسط کاربر می‌باشد. در قسمت کلاینت، مسئله یا تصویر ارسالی از طرف سرور را دریافت و به کاربر نمایش می‌دهد و پاسخ تولیدشده را به سرور ارسال می‌نماید.

جهت ارزیابی تصدیق‌کننده ای‌پی‌آی به بررسی این سیستم جهت مقابله با حملات اسپوفینگ مک‌آدرس، کلاهبرداری از تصدیق‌کننده ای‌پی‌آی کلاینت و عبور کردن از تایید کننده کپچا پرداخته و جهت بررسی کپچای پیشنهادی به بررسی آن در مقابل حملات بروت‌فورس، رلی وتشخیص تصاویر می‌پردازیم.

دراین فصل شرح موضوع و زمینه پژوهش، سئوالاتی که محقق در جستجوی پاسخ آنهاست، اهداف وسوابق تحقیق، فرضیه‌های پژوهشی و ساختار تحقیق بیان خواهدشد.

۱-۱) تعریف مساله و کلیات تحقیق

بات[1] یک برنامه نرم‌افزاری است که به اجرای دستورات ارسالی از طرف بات‌مستر می‌پردازد. باتنت شبکه‌ای از کامپیوترها(بات‌ها) است که از راه دور توسط یک مهاجم و از طریق کانال‌های از پیش تعریف شده دستور و کنترل[2] نظیرای‌ارسی[3]، پی‌توپی[1] و یا

[1] Bot
[2] Command and Control
[3] Internet Relay Chat(IRC)

پروتکل‌های مبتنی بر وب کنترل می‌شوند. از جمله حملات باتنت‌ها می‌توان به حملات دی داس[۲]، اسپمینگ[۳]، ترافیک اسنیفینگ[٤]، پیشینگ وسرقت هویت اشاره نمود.(مک کارتی[٥]،۲۰۰۳)

این نوع از حملات می‌توانند به طور مستقل و یا به همراه حملات ویروسی و یا کرم‌های[٦] رایانه‌ای رخ دهند. همراهی این نوع حملات با ویروس‌های رایانه‌ای علاوه بر پیچیدگی مقابله، ضررحاصل شده به اهداف مورد نظر را به طرز چشمگیری افزایش می‌دهد. به عنوان مثال در سال ۲۰۰٦ شرکت های ارائه دهنده اکانت ایمیل با رشد بسیار چشمگیری در ارسال ایمیل‌های ناخواسته(اسپم) مواجه گردیدند.

اسپم‌ها به عنوان یکی از اشکال باتنت نقش بسیار مهمی در جرایم سایبری بر عهده دارند. علیرغم اینکه شرکت‌های پیشرو در صنعت فناوری اطلاعات نظیر مایکروسافت هرروزه ابزارهای جدیدتری را برای مبارزه با اسپم‌ها تولید می‌کنند امروزه شاهد رشد گسترده اسپم‌ها می‌باشیم.

عمده‌ترین واصلی‌ترین دلیل ارسال اسپم‌ها سودآوری آنها است. اسپم ارزان‌ترین روش ارسال تبلیغات به کاربران تجهیزات رایانه‌ای و بدست آوردن اطلاعات خصوصی آنها است. اسپم‌ها علاوه برتبلیغات جهت آلوده‌سازی رایانه‌ها به بدافزارها نیز مورد استفاده قرار می‌گیرند. درسال ۲۰۰۹ که صنعت رایانه دچار افول قابل توجهی گردیده بود گروهی از تولید کنندگان اسپم روسی، اسپمی به نام ویاگرا[۷] را طراحی کرده و از طریق آن روزانه ٤۰۰۰ دلار سود حاصل نمودند.(والش[۸]،۲۰۰۹)

بر طبق مطالعات صورت گرفته در سایت اسپم هاوس[۹] در سال ۲۰۱۰ باتنت‌ها علت انتشار ۹۵٪ مجموع اسپم‌های ارسالی می‌باشند. بر اساس آمار ارائه شده در سایت میل شاین[۱۰]

[1] Peer to Peer
[2] DDOS
[3] Spamming
[4] Traffic Sniffing
[5] McCarty
[6] Worm
[7] Viagra
[8] Walsh
[9] Spamhaus
[10] Mailshine

نتیجه فعالیت‌های اسپم‌ها در سال ۲۰۱۰ضرری در حدود ۱۰۳ بیلیون دلار به جامعه جهانی بوده‌است.(اسپم هاوس،۲۰۱۰)

عدد قابل توجه فوق بر اساس محاسبات ذیل محاسبه گردیده است:

- تعداد ایمیل‌های سالانه ارسال شده ۱۰۷ تریلیون ایمیل می‌باشد.
- تعداد ایمیل‌های اسپم ارسالی ۹۵ تریلیون ایمیل در سال ۲۰۱۰ می‌باشد.
- میانگین زمانی که هر فرد صرف یک اسپم می کند نیم‌ثانیه می‌باشد.
- میانگین دستمزد هر فرد ۱۰ دلار در ساعت است.

سوالی که پیش می‌آید عبارت است از اینکه باتنت‌ها به چه میزان امنیت سایبری را تهدید می‌کنند؟ تعیین تعداد رایانه‌های که به اینترنت متصل بوده و به بات آلوده هستند به سختی امکان پذیرمی‌باشد و تعداد آنها نیز به طور مداوم در حال افزایش است. در سال ۲۰۰۹ شرکت مک آفی[1] تعداد رایانه‌های آلوده به بات را ۱۵۰ هزار تخمین زده بود در حالی که در سال ۲۰۰۷ شرکت سیمانتک تعداد کامپیوترهای آلوده را ۵۰ هزار رایانه برآورد نمود و این به معنی سه برابر شدن تعداد رایانه‌های آلوده ظرف مدت دو سال می‌باشد. بر طبق آماری که در سال ۲۰۱۰ توسط شرکت بردلب[2] منتشر گردید بر روی کامپیوترهای آلوده بیش از ۳۰ میلیون بات وجود دارد. آنچه واضح است حضور بات‌ها به تنهایی تهدید بسیار جدی برای امنیت جهانی اینترنت می‌باشد.

طراحان بدافزارها از باتنت به منظور حملات دی داس نیز استفاده می‌نمایند. منظور از این حملات ارسال درخواست به یک یا چند سرور به خصوص از طریق هزاران کامپیوتر در سرتاسر شبکه می‌باشد که باعث قطع شدن سرویس مربوطه می‌گردد. با توجه به اینکه بات‌ها در سرتاسر اینترنت گسترده می‌باشند شناسایی منبع این حملات بسیار مشکل است. ترافیک اینترنت نیز در سراسر شبکه بطور عادی بوده و تنها در نزدیکی این سرورها ترافیک به صورت غیره منتظره‌ای به سمت سرور مربوطه همگرا می‌گردد. با توجه به اینکه این حملات از محل‌های مختلفی صورت می‌گیرد شناسایی و جلوگیری از آنها نیاز به

[1] MacAfee
[2] Bredlab

همکاری مدیران امنیتی شبکه‌ها در محل‌های مختلف و متفاوت در سراسر جهان می‌باشد. شناسایی بات‌ها یک راه حل است. اما روش بهتر و موثرتر، شناسایی بات مستر و یا افرادی است که در پشت این حملات قرار دارند. باتوجه به اینکه از کامپیوترهای اشخاص مختلف به منظور حملات استفاده می‌گردد شناسایی بات‌مستر امری بسیار مشکل است.(وال فیش[1]،۲۰۰۶)

در دهه اخیر باتنت‌ها در صنایع مختلفی رشد پیدا کرده‌اند. بر اساس آخرین مطالعات انجام شده توسط شرکت پونمون[2] در ۵۰ شرکت آمریکایی که قربانی حملات باتنت بودند میانگین ضرر سالیانه هر شرکت حدود ٦ میلیون دلار می باشد. بر اساس آمار این شرکت میزان ضرر حاصل از فعالیت های خرابکارانه باتنت‌ها و همچنین هزینه جلوگیری از فعالیت‌های باتنت‌ها به طور چشمگیری در حال افزایش است.(پونمون،۲۰۱۱)

یکی از متداولترین انواع اسپم‌ها پیشینگ می‌باشد. پیشینگ روش فریبکارانه‌ای است تا کاربران اطلاعات مورد نیاز جهت دسترسی به کارت‌های اعتباری و بانکی خود را ارسال نمایند. از نام کاربری و رمزکاربران که با استفاده از تکنیک پیشینگ بدست می‌آید به منظور خریدهای آنلاین، برداشت پول نقداز حساب و یا انتقال به سایر حساب‌ها استفاده می‌گردد. به عنوان مثال براساس گزارشات منتشرشده یک حمله ساده طراحی شده به موسسه مالی یو اس [3]روزانه به طور متوسط ۵۰ هزار دلار از طریق کاستن ۵۰ دلار از موجودی اکانت هر یک از کاربران به آن موسسه زیان رساند.(مک آفی[4]،۲۰۰۹)

رشدگسترده باتنت‌ها ناشی از طبیعت آنها می‌باشد که بسیار سریع گسترده می‌شوند. یک مجموعه از بات‌ها که در زیر نظر یک بات‌مستر به طور مستقل کار می‌کنند می‌توانند روزانه میلیون ها اسپم تولید نمایند. نکته قابل توجه این است که جلوگیری از رشد باتنت‌ها بسیار مشکل است. طراحان این بدافزارها روش‌های مختلفی را بکار می‌برند تا عملکرد بات‌ها را از نظر کاربران مخفی نگهدارند. هنگامی که یک کامپیوتر به یک بات آلوده می‌گردد عملکردش با زمانی که آلوده نشده است فرقی ندارد. این نکته فرق مهم میان بات و ویروس می‌باشد. یعنی وقتی سیستم به ویروس آلوده‌شد عملکردش بطور قابل توجهی کند

[1] Walfish
[2] Ponemone
[3] US financial Institution
[4] McAfee

می‌شود در صورتی که هنگام آلوده‌شدن به بات تا ارسال دستور از طرف بات‌مستر هیچ فعالیتی از خود نشان نمی‌دهد. بات‌ها به منظور کاهش امکان شناسایی تنها در زمان مورد نیاز فعال می‌شوند و در حال عادی غیرفعال می‌باشند.

اولین و مهمترین گام در مقابله با باتنت‌ها شناسایی آنها می‌باشد. روش‌های شناسایی بدافزارها به دو دسته ذیل قابل تقسیم بندی است:

۱- شناسایی رفتارهای غیر متعارف[1]: هدف شناسایی فرآیندهایی است که به طور غیرعادی رفتار می‌کنند. این روش شناسایی زمانی مفید است که از نحوه رفتار و اثرات یک فرآیند در حالت عادی اطلاع داشته باشیم.(برینکلی[2]،۲۰۰۶)

۲- شناسایی از طریق استفاده‌های نامناسب[3]: به بررسی فرآیندهایی می‌پردازد که رفتارهای غیرمجاز دارند و سعی به دسترسی به اطلاعات و نواحی که نمی بایستی به آن دسترسی داشته باشند را دارند.

شناسایی سیستم‌های بدافزار در دو حوزه قابل بررسی می‌باشد:

سیستم‌های بر پایه هاست[4]: سیستم‌های که فرآیندها را بررسی می‌نمایند و فعالیت آنها را بطور محلی بررسی نموده تا پراسس‌هایی که رفتارهای غیر قانونی(غیر مجاز)را دارند شناسایی نمایند.

سیستم‌های بر پایه شبکه[5]: سیستمهای می‌باشند که شبکه را کنترل نموده و با آنالیز ترافیک، فرآیندهایی که در شبکه ایجاد ترافیک غیرضروری می‌نمایند را شناسایی می‌کنند.

باتنت۲ نسل جدیدی از باتنت‌ها است که زیر ساخت‌های وب۲ را تحت کنترل درآورده و از طریق ایجاد کانال دستور و فرمان به سرقت اطلاعات و ارسال دستورات جهت بات‌ها استفاده می‌نماید.

یک باتنت شامل دوجزء اصلی ذیل است:

[1] Anomaly Detection
[2] Brinkley
[3] Misuse Detection
[4] Host Based System
[5] Network Based System

بات: یک برنامه نرم‌افزاری بوده که به اجرای دستورات ارسالی از طرف بات‌مستر می‌پردازد.

بات مستر: یک هکر می‌باشد که فعالیت بات‌ها را هماهنگ کرده و دستوراتی را جهت انجام به بات‌ها ارسال می‌نماید.

ارتباط بات و بات‌مستر از طریق کانال دستور و فرمان بوده که بر روی بستر سرویس‌های وب۲ انجام می‌پذیرد. با راه اندازی کانال‌های دستور و فرمان موارد ذیل صورت می‌پذیرد:

۱- بات‌مستر یک پروفایل برروی یک سرویس و بلاگ عمومی یا یک سایت شبکه اجتماعی ایجاد نموده واز این پروفایل جهت ارسال دستورات و بروز کردن بات‌ها استفاده می‌نماید.

۲- کاربران شبکه از طریق اراس‌اس[1] از بروز شدن بلاگ یا وب سایت آگاه می‌شوند. بات‌ها نیز به همین طریق(استفاده از اراس‌اس) از دستورات جدید مطلع می‌گردند.

۳- پس از اطلاع بات‌ها از بروز شدن اطلاعات توسط اراس‌اس‌ها، اطلاعات و فایل‌های مربوطه توسط بات‌ها از پروفایل دانلود و اجرا می‌گردد.

٤- اطلاعات مورد نظر از روی سیستم قربانیان برداشته شده و در پروفایل مربوطه آپلود می‌گردد.

۵- بات‌مستر از طریق اراس‌اس ازآپدیت شدن اطلاعات توسط بات‌ها مطلع می‌گردد.

با توجه به اینکه باتنت۲ از سرویس‌های که در دسترس همگان می‌باشد استفاده می‌کنند، ترافیک ایجاد شده جهت برقراری ارتباط میان بات و بات‌مستر جزء ترافیک عمومی وب خواهد بود. بنابراین اغلب نرم‌افزارهای طراحی شده جهت مقابله با بدافزارها، امکان تشخیص ترافیک ایجاد شده توسط بات‌ها را ندارند. لازم به ذکر است بات و بات‌مستر اطلاعاتی را بین خود به طور مستقیم جابجا نمی‌کنند بلکه دیتا از طریق دستگاههای ذخیره سازی عمومی جابجا می‌شوند.

مثال‌هایی از این بات‌های۲ عبارتند از:

[1] RSS

تویتربات[1]: اولین بات شناسایی شده است که ازپروفایل تویترجهت ارسال دستورات باتمستر به باتها استفاده می‌نماید. این بات همچنین از تویتر اراس‌اس [2]به منظوراطلاع به باتها از آماده بودن دستورات استفاده می‌کند.(نازاریو[3]،۲۰۰۹)

وایت ول تروجان[4]: این بات از اکانت فیس‌بوک به منظور هماهنگ کننده سرورهای دستور و فرمان استفاده می‌نماید. همچنین دستورات پیکربندی را از طریق اکانت فیس‌بوک دریافت نموده و این دستورات را از طریق وب سرورها توزیع می‌نماید.

تروجان گروه گوگل[5]: این بات ازگروه‌های گوگل برای توزیع دستورات استفاده می‌کند. باتمستر یک اکانت و یک صفحه شامل دستورات مورد نظر برای بات‌ها را ایجاد می‌نماید. یک دستور علاوه بر فرمانی که می‌بایستی اجرا شود شامل فایلی است که می‌بایستی دانلود گردد. وقتی یک تروجان اجرا می‌گردد به یک اکانت از پیش تعریف شده وصل گردیده و اطلاعات و دستورات را کسب و اجرا می‌کند.(گورمن[6]،۲۰۰۹)

۱-۲) سوالات اصلی تحقیق

مساله اصلی در این تحقیق را می‌توان بصورت زیر عنوان کرد:

چگونه می‌توان با استفاده از تصدیق‌کننده رابط برنامه کاربردی[7] و کپچا از سوءاستفاده از سرویس‌های وب جلوگیری نمود؟

جهت بررسی مساله اصلی تحقیق باید به سوال‌های اصلی تحقیق که به شرح ذیل می‌باشند پاسخ داد:

۱- تصدیق‌کننده رابط برنامه کاربردی چگونه می‌تواند ضمن شناسایی باتنت‌ها از ارتباط میان بات با باتمستر جلوگیری کند؟

۲- با استفاده ازکپچای بهبودیافته چگونه می‌توان از انتشارباتنت‌ها جلوگیری نمود؟

[1] Twitter Bot
[2] Twitter RSS
[3] Nazario
[4] White Well Trojan
[5] Google Group Trojan
[6] Gorman
[7] Application Programming Interface (API)