فصلنامه رویکردهای نوین در تحقیقات علوم پایه، فنی و مهندسی
سال پنجم، شماره ۱۹ ،زمستان ۱۴۰۱
ISSN: ۲٦٤٥-٥٤٣٩
www.jonarbset.ir

بررسی نحوه عملکرد باتنت‌های مبتنی بر کانال‌های پنهان

مینا صاحبی [۱]

[۱] کارشناسی ارشد مهندسی فناوری اطلاعات دانشگاه آزاد قزوین

چکیده

امروزه باتنت‌ها یکی از مهم‌ترین تهدیدات در برابر زیرساخت اینترنت شناخته می‌شوند. هر باتنت گروهی از میزبان‌هایی است که با کد مخرب یکسانی آلوده‌شده و از طریق یک یا چند سرویس‌دهنده فرمان و کنترل توسط مهاجم از راه دور هدایت می‌شوند. همزمان با ارائه پیشنهادهای جدید برای شناسایی باتنت‌ها، مهاجمین از روش‌های مقاوم‌تری جهت عدم شناسایی باتنت خود استفاده می‌کنند. از آن‌جایی که با شناسایی کانال‌های فرمان و کنترل به آسانی می‌توان باتنت‌های مختلف را متلاشی کرد، شناسایی این کانال‌ها در روش‌های تشخیص باتنت از اهمیت زیادی برخوردار است. مهاجمین با هدف افزایش طول عمر باتنت‌های خود از استراتژی‌های متفاوتی برای ایجاد کانال‌های فرمان و کنترل استفاده می‌کنند. از این‌رو باتنت‌های مختلف با سازوکارهای مختلفی ایجاد شده‌اند. در این پژوهش سعی شده است که به بررسی انواع مختلف کانال‌های فرمان و کنترل در باتنت‌ها و روش‌های مختلفی که مهاجمان از آن برای کنترل باتنت‌های خود استفاده می‌کنند، پرداخته و روش‌های مختلفی را که برای تشخیص این نوع باتنت‌ها معرفی شده اند بیان شود.

واژه‌های کلیدی: باتنت، کانال فرمان و کنترل، کانال پنهان، تشخیص باتنت.

۱. مقدمه

با گسترش روزافزون شبکه‌های کامپیوتری و ازدیاد حجم اطلاعات مورد مبادله در آن‌ها، امنیت شبکه به یک چالش بزرگ برای مدیران شبکه تبدیل شده است. همزمان با سیر پیشرفت فن‌آوری اطلاعات و ارائه خدمات نوین اینترنتی توسط مؤسسات و شرکت‌های مختلف خصوصی و دولتی، مهاجمین نیز از عواملی چون ناآگاهی کاربران و آسیب‌پذیری‌های مختلف موجود در نرم‌افزارها سوءاستفاده کرده و مشکلاتی را برای کاربران ایجاد کرده‌اند. در حال حاضر امنیت در 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 شناسایی شدن توسط سیستم‌های تشخیص نفوذ جلوگیری کنند. حملات اینترنتی با انگیزه‌های مختلفی از قبیل کسب شهرت و درآمد، سرگرمی، خراب‌کاری و اهداف سیاسی انجام می‌شوند. در چند سال گذشته، اهداف و جهت‌گیری این تهدیدات به طور قابل ملاحظه‌ای تغییر یافته و به سمت سازماندهی بهتر و سود محوری بیشتر تکامل پیدا کر ده‌اند [۱].یکی از مهم‌ترین ویژگی سرویس‌دهنده‌های اینترنتی دسترس‌پذیری همیشگی آن‌ها است. در صورت عدم دسترس‌پذیری یک سرویس‌دهنده، سرویس مورد نظر قابل ارائه به کاربران نمی‌باشد. به عنوان مثال، در سال ۲۰۰۸ فروشگاه آنلاین آمازون در حدود ۲ ساعت غیرقابل دسترس شد. به دلیل این اتفاق، علاوه بر این‌که ضرری در حدود ۳۱،۰۰۰ دلار در هر دقیقه به این فروشگاه وارد شد، ارزش سهام آن نیز ۴،۱ درصد کاهش یافت. یک مهاجم می‌تواند با در اختیار داشتن باتنتی که حدود ۱۰۰۰ تا ۲۰۰۰ بات داشته باشد یک حمله جلوگیری از سرویس توزیعی را بر روی هر سرویس‌دهنده اینترنتی اجرا کند و خسارات جبران ناپذیری را وارد نماید [۲].

تعداد باتنت‌ها در چند سال اخیر به طور چشمگیری رشد کرده و به عنوان یکی از خطرناک‌ترین تهدیدات بدافزاری تبدیل شده است که مسئول حجم عظیمی از رفتارهای بدخواهانه در اینترنت است [۱]. بیشتر کاربران اینترنتی، اغلب از به تصرف در آمدن میزبان‌های خود و قرار گرفتن در بخشی از یک باتنت بی‌اطلاع هستند. همچنین بات‌هایی که اختیار میزبان‌های به تصرف درآمده را در دست می‌گیرند، قادر هستند تا با استفاده از روش‌های مبهم‌سازی از کشف شدن توسط آنتی‌ویروس‌های معمول بگریزند. بنابراین، همواره نیاز به توسعه یک روش اختصاصی برای تشخیص باتنت‌ها وجود دارد.

در سال‌های اخیر روش‌های متعددی برای تشخیص باتنت‌ها مبتنی بر شناسایی ترافیک کانال‌های فرمان و کنترل پیشنهاد شده است. همزمان با ارائه پیشنهادهای جدید برای شناسایی باتنت‌ها، مهاجمین از روش‌های مقاوم‌تری جهت عدم شناسایی باتنت خود استفاده می‌کنند .

در این پژوهش مطالبی به منظور آشنایی با باتنت‌ها برای ورود به بحث اصلی بیان می‌شود. ابتدا مفاهیم مرتبط با باتنت‌ها توضیح داده شده و انواع باتنت‌ها معرفی می‌شوند. سپس کانال‌های فرمان و کنترل به عنوان یک ویژگی متمایز کننده باتنت‌ها معرفی شده و بر اساس ساختار و پروتکل آن‌ها انواع باتنت‌ها بیان می‌شود. در ادامه چرخه حیات باتنت شامل شکل‌گیری، فرمان و کنترل، و حمله به تفصیل شرح داده می‌شود.

۲. مفاهیم بات نت ها و انواع آن ها

هر باتنت یک گروه هماهنگ از بات‌هایی است که از طریق کانال‌های فرمان و کنترل هدایت شده و فعالیت‌های مخربی را انجام می‌دهند[۳]. عبارت "گروه هماهنگ" از بات‌ها به این معنا است که چندین بات عضو یک باتنت، فرامین یکسانی را دریافت کرده و فعالیت‌های مخرب مشابهی را انجام می‌دهند. عبارت "هدایت شده" به معنای آن است که بات‌ها برای انجام دادن فعالیت‌های خود نیاز دارند تا با سرویس دهندگان فرمان و کنترل ارتباط برقرار کرده و فرامین مدیر بات را از طریق آن‌ها دریافت نمایند. به عبارت دیگر می‌بایست ارتباطی بین بات‌ها و سرویس‌دهندگان فرمان و کنترل وجود داشته باشد .

واژه بات از روبات برگرفته شده است. همانند روبات‌ها، بات‌ها برای انجام برخی از عملیات از پیش تعریف شده طراحی شده اند، که به صورت خودکار انجام می‌شوند[۴]. یک بات، که با نام زامبی شناخته می‌شود، بدافزاری است که بر روی یک میزبان (آسیب‌پذیر که به تصرف مهاجم در آمده است) اجرا شده و فرامین دریافتی از مهاجم را به انجام می‌رساند[۵]. در عمل، بات‌ها نوعی ویروس و کرم اینترنتی هستند که یک میزبان آسیب‌پذیر را آلوده کرده و قابلیت ارتباط از راه دور با مهاجم را برای دریافت فرامین وی فراهم می‌کند. در تقابل با بدافزارهای موجود مانند ویروس‌ها و کرم‌های اینترنتی که هدف اصلی آن‌ها تنها انجام فعالیت مخرب است در میزبان آلوده، بات‌ها به طور معمول برای راه‌اندازی حملات مختلف بر روی سایر قربانیان نیز به کار می‌روند. به عبارت دیگر، مهاجم قادر است تا انواع مختلفی از حملات را به صورت هماهنگ و با قدرت تخریبی بسیار بالا بر روی سایر قربانیان سازماندهی کند، در حالی‌که به طور معمول هویت وی مخفی می‌ماند.

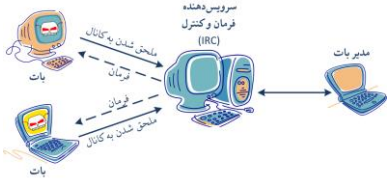
هر باتنت شامل سه قسمت اصلی است: مدیر بات ، بات و کانال فرمان و کنترل. مدیر بات فرد مهاجم است که باتنت خود را با فرامین مختلف از راه دور هدایت می‌کند. به مدیر بات همچنین چوپان بات نیز می‌گویند. مدیر بات می‌تواند از توان پردازشی میزبان‌های به تصرف در آمده به صورت توزیعی به نفع خود بهره‌برداری کند. بات به این صورت طراحی شده است که میزبان‌ها را آلوده کند و میزبان‌های آلوده‌بخشی از باتنت می‌شوند بدون اینکه قربانی اطلاعی پیدا کند و شبکه باتنت تحت نظارت مدیر بات کنترل می‌گردد. مدیر بات دستورات را برای تمامی بات‌ها در شبکه ارسال می‌کند و آن‌ها را از طریق کانال‌های فرمان و کنترل هدایت می‌کند[.۶]

تشخیص باتنت به مجموعه‌ای از فعالیت‌ها و روش‌هایی گفته می‌شود که یک مدافع برای شناسایی میزبان‌های آلوده به بات به کار می‌گیرد. هدف از تشخیص باتنت از کارانداختن و یا سبک کردن تهدیدات ناشی از یک باتنت است .

بات نت ها به دو نوع تقسیم میگردند: بات نت های متمرکز و بات نت های غیر متمرکز. در باتنت‌های متمرکز مدیر بات یک میزبان با پهنای باند بالا را به عنوان نقطه مرکزی (سرویس‌دهنده فرمان و کنترل) برای همه بات‌ها انتخاب می‌کند. سپس بر روی این میزبان، سرویس‌های شبکه‌ای خاصی (از قبیل آی‌آرسی یا اچ‌تی‌تی‌پی) را برای برقراری ارتباط با بات‌ها اجرا کرده و از این طریق باتنت خود را هدایت می‌کند.

استفاده از این نوع باتنت‌ها مزایایی از قبیل دسترس‌پذیری بالا، برقراری ارتباط آسان با بات‌ها، تأخیر کم در ارسال پیام‌ها به بات‌ها و کنترل ساده‌تر باتنت را دارد. اما برپایی چنین باتنتی یک ضعف عمده دارد و آن نقطه یگانه شکست بودن سرویس‌دهنده فرمان و کنترل است، یعنی از آنجایی‌که تمامی ارتباطات در باتنت با استفاده از این سرویس‌دهنده انجام می‌شوند، در نتیجه کشف شدن و از کار افتادن آن، ارتباط بین بات‌ها و مدیر بات از بین رفته و کل باتنت از کار می‌افتد [۱]. این بات نت ها به دو نوع مبتنی بر آی آر سی و مبتنی بر اچ تی تی پی تقسیم می شوند.

آی‌آرسی پروتکلی برای پیام‌رسانی مبتنی بر متن بی‌درنگ و یا برپایی کنفرانس هم‌زمان بر روی اینترنت است [۷]. هر سرویس‌دهنده آی‌آرسی کانال‌های گفت‌وگوی متنوعی را برای کاربران میزبانی می‌کند. در باتنت‌های مبتنی بر آی‌آرسی، مدیر بات کانالی را در سرویس‌دهنده آی‌آرسی ایجاد کرده تا فرامین خود را در آن پست کند. سپس بات‌ها در این کانال عضو می‌شوند و یک نام کاربری منحصر به فرد به هر باتی تعلق می‌گیرد. مدیر بات دستورات خود را روانه این کانال‌ها می‌کند و هر بات متصل به آن کانال دستورات را دریافت می‌نماید .شکل ۱ نمایی از باتنت با ساختار متمرکز مبتنی بر آی‌آرسی را نمایش می‌دهد. ***[۹]***



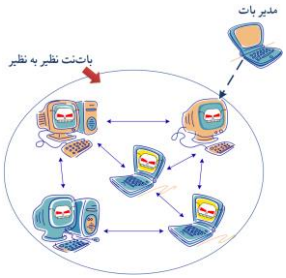
شکل ۱ نمایی از یک باتنت با ساختار متمرکز مبتنی بر آی‌آرسی[۹]

در یک باتنت مبتنی بر اچ‌تی‌تی‌پی، ابتدا مدیر بات یک سرویس‌دهنده وب برپا کرده و فرامین خود را در آن قرار می‌دهد. سپس بات‌ها به طور دوره‌ای به این سرویس‌دهنده متصل شده تا جدیدترین فرامین را دریافت کنند. یکی از مزیت‌های این نوع بات مخفی ماندن ترافیک فرمان و کنترل باتنت در میان ترافیک اچ‌تی‌تی‌پی معمول مرور کاربران از صفحات وب است .

اگرچه به راحتی می‌توان باتنت‌هایی با ساختار متمرکز ایجاد نمود، اما این ساختار دارای یک ضعف عمده است. سرویس‌دهنده فرمان و کنترل نقطه یگانه شکست است. از کار انداختن این سرویس‌دهنده باعث خواهد شد تا مدیر بات ارتباط خود با همه بات‌ها را از دست بدهد.در باتنت‌های غیرمتمرکز برای از بین بردن ضعف نقطه یگانه شکست، زیرساخت ارتباطی به طور کامل بر روی تنها یک و یا چند سرویس‌دهنده فرمان و کنترل استوار نیست. همچنین در این حالت با شناسایی تعدادی از میزبان‌های آلوده به بات، نمی‌توان کل باتنت را از کار انداخت. هر باتی در این نوع باتنت می‌تواند هم به عنوان سرویس‌دهنده و هم به عنوان سرویس‌گیرنده عمل کند. از آنجایی‌که در این نوع باتنت‌ها یک سرویس‌دهنده مرکزی وجود ندارد، کشف و از کارانداختن شبکه باتنت بسیار مشکل و پیچیده است. از معایب این نوع باتنت می‌توان به مواردی همچون تأخیر انتشار دستورات بین بات‌ها، نبودن تضمین جهت رسیدن دستورات به تمام بات‌ها و مدیریت سخت‌تر آن‌ها اشاره کرد.

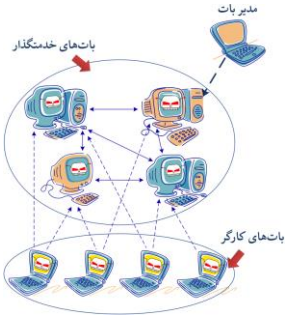
باتنت‌های غیرمتمرکز را می‌توان به دو نوع توزیعی (نظیر به نظیر) و ترکیبی تقسیم نمود.

در این نوع باتنت‌ها، مدیر بات از یک پروتکل نظیر به نظیر برای برقراری ارتباط با بات‌های خود استفاده می‌کند. شکل ۲ نمایی از باتنت با ساختار غیرمتمرکز نظیر به نظیر را نمایش می‌دهد . ***[۱۰]***



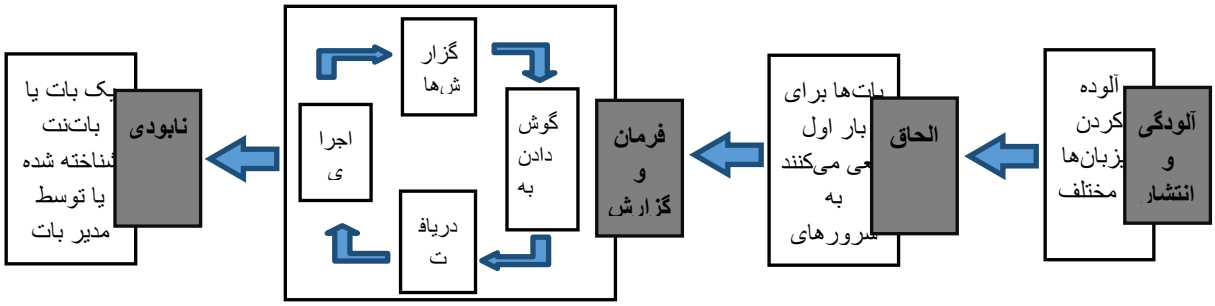
شکل ۲ نمایی از یک باتنت با ساختار غیرمتمرکز نظیر به نظیر[۱۰]

در این نوع باتنت‌ها، هر بات به جای اتصال به یک سرویس‌دهنده فرمان و کنترل مرکزی به بات‌های همتای خود متصل شده و هم‌زمان به عنوان متقاضی و سرویس‌دهنده عمل می‌کند. بنابراین اگر برخی از بات‌ها در یک باتنت تشخیص داده شوند، آن باتنت هم‌چنان می‌تواند به فعالیت‌های خود تحت هدایت مدیر بات ادامه دهد. مدیر بات فرامین خود را در اختیار یک یا چند بات برگزیده قرار داده و آن‌ها این فرامین را در شبکه نظیر به نظیر پخش می‌کنند تا همه بات‌ها فرامین جاری وی را در اختیار داشته باشند. به طور معمول بات‌ها برای دریافت فرامین از یک کلید برای جستجو استفاده کرده تا فرامین جاری شاخص شده را دریافت نمایند.باتنت‌های ترکیبی هر دو ساختار متمرکز و توزیع‌شده را با یکدیگر ترکیب کرده و یا از یک ساختار تصادفی استفاده می‌کنند تا خودشان را در مقابل تشخیص مقاوم‌تر سازند. جهت درک بهتر این ساختار مثالی در شکل۳ آورده شده است.



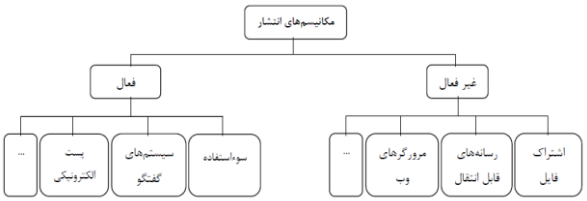
شکل ۳ نمایی از یک بات‌نت با ساختار غیرمتمرکز ترکیبی[۱۱]

با توجه به این شکل دو گروه از بات‌ها وجود دارند: خدمت‌گزار و کارگر. خدمت‌گذار بات‌هایی هستند که دارای آدرس‌های آی‌پی ایستای عمومی بوده و به هر دو صورت متقاضی و سرویس‌دهنده عمل می‌کنند و همچنین از طریق اینترنت نیز در دسترس می‌باشند. آن‌ها از اتصالات نظیر به نظیر استفاده کرده و فرامین مدیر بات را برای متقاضیان بازپخش می‌کنند. در سوی دیگر، متقاضیان بات‌هایی با آدرس‌های آی‌پی پویای خصوصی بوده که در پشت دیواره‌های آتش و یا ادوات نَت قرار دارند که نمی‌توانند اتصالات ورودی از اینترنت را بپذیرند. آن‌ها همیشه به بات‌های خدمت‌گزار متصل شده تا فرامین جدید را به‌دست آورند [۱۱]. برخلاف سایر بدافزارها، بات‌نت‌ها چرخه حیات شفاف‌تری دارند که می‌تواند به سه مرحله اصلی آلودگی و شکل‌گیری، فرمان و کنترل و حمله تقسیم شود. در هر مرحله نوع فعالیت بات‌نت‌ها متفاوت است.در شکل ۴ چرخه حیات بات نت نشان داده شده است.



شکل ۴ چرخه حیات بات‌نت[۸].

مکانیزم‌های انتشار می‌توانند به دو دسته فعال و غیرفعال تقسیم شوند. اگر برنامه بات، توسط برنامه بات در حال اجرا منتشر شود، نوع انتشار آن فعال و در غیراین‌صورت نوع انتشار آن غیرفعال خواهد بود. در شکل ۵ مکانیزم‌های انتشار معمول نمایش داده شده است.

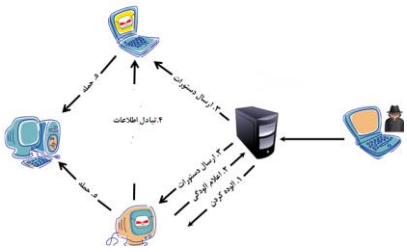


شکل ۵ انواع مکانیزم‌های انتشار

به منظور پیاده‌سازی یک سیستم دفاعی مؤثر در مقابل بات‌نت‌ها، لازم است که چگونگی عملکرد بات‌نت‌ها را به درستی درک نمائیم. شکل ۶ نحوه عملکرد یک بات‌نت را نشان می‌دهد.

۱-در ابتدا میزبان‌های آسیب‌پذیر به یک کد مخرب آلوده می‌شوند. این کدهای مخرب به طور معمول با استفاده از رمزگذاری مبهم‌سازی می‌شوند تا بر سیستم‌های تشخیص نفوذ مبتنی بر امضاء غلبه کنند. بر اثر اجرای این کد در سیستم

قربانی، بات خودش را از حالت مبهم خارج می‌کند و تعدادی فراخوانی‌های سیستمی را اجرا کرده تا خود را پنهان نماید (به عنوان مثال با تغییر در فایل‌های سیستمی یا اضافه کردن خود به سرویس‌های سیستمی قانونی). بات در سیستم قربانی شروع به جمع‌آوری اطلاعات مهم از قبیل نام‌های کاربری و پسورد و یا اطلاعات کارت‌های اعتباری می‌کند.



شکل ۶ نحوه عملکرد یک بات‌نت

۲-در این مرحله بات به سرویس‌دهنده فرمان و کنترل متصل می‌شود تا عضوی از بات‌نت شود.

۳-هم‌زمان که بات دستورات جدید را از سرویس‌دهنده فرمان و کنترل دریافت می‌کند اطلاعات جمع‌آوری شده خود را برای آن ارسال می‌کند و نسخه جدید بدافزار خود را دانلود می‌نماید.

۴-بات با استفاده از کاوش در شبکه محلی خود سعی در آلوده کردن میزبان‌های دیگر داشته یا فایل بدافزار خود را به پست‌های الکترونیکی پیوست کرده و برای مخاطبین کاربر آلوده ارسال می‌کند. به این ترتیب تعداد بات‌های عضو بات‌نت به مرور زمان بیشتر شده و بات‌نت در شبکه گسترش می‌یابد.

۵- پس از این‌که تعداد میزبان‌های آلوده به اندازه کافی رسیدند، مدیر بات می‌تواند با دستور دادن به این بات‌ها حملات متعددی را انجام دهد. باید توجه داشت که بات‌نت‌ها در طی انجام این حملات می‌توانند همچنان گسترده‌تر شوند. در واقع مدیربات می‌تواند از بات‌نت خود علاوه بر انجام حملات متنوع، برای گسترش بات‌نت خود نیز استفاده کند. **[۱۴]**

۳. کانال پنهان

کانال پنهان به معنی مبادله اطلاعات در پوشش یک کانال آشکار و مجاز است به نحوی که اصل وجود ارتباط مخفی بماند. کانال‌های پنهان دارای کاربردهای زیادی برای مقاصد مجاز یا بدخواهانه است که محور همه آن‌ها برقراری ارتباط پنهان بین منابع انسانی یا نرم‌افزاری در فضای اینترنت است. کانال‌های پنهان از پروتکل‌هایی که برای ارتباطات مجاز برقرار است، برای سوار کردن اطلاعات پوششی و مبادله اطلاعات بین منابع استفاده می‌کند. کانال‌های پوششی دارای سه معیار ارزیابی ظرفیت، استحکام و نامحسوسی می‌باشند.برای کانال پوششی تعاریف مختلفی ارائه شده است:

-لامپسون [۱۲] کانال پنهان را یک کانال ارتباطی می‌داند که برای انتقال اطلاعات استفاده می‌شود، ولی به طور کلی نه برای ارسال اطلاعات طراحی شده و نه مقصود آن بوده است.

- در فرهنگ اصطلاحات وزارت دفاع امریکا [۱۳] کانال پنهان یک کانال ارتباطی است که می‌تواند توسط پردازه‌ای برای ارسال اطلاعات استفاده شود به نحوی که از سیاست امنیت تشکیلات تجاوز نماید.

-در [۲۸] کانال پنهان یک کانال ارتباطی انگلی است که به منظور ارسال اطلاعات بدون اجازه یا آگاهی طراح، مالک یا اپراتور کانال، از پهنای باند آن استفاده می‌کند.

این تعاریف از این جهت مهم است که حقیقت ذاتی و منظور کانال‌های پنهان را آشکار می‌سازد، یعنی عبور از سیاست امنیت تشکیلات و ارسال اطلاعات به صورت پنهان بدون آنکه تشخیص داده شود. روش‌های زیادی برای قرار دادن اطلاعات در بخش‌های بدون استفاده برخی از پروتکل‌های شبکه مانند آی‌پی، تی‌سی‌پی و غیره وجود دارد. علاوه بر پروتکل‌های شبکه، امروزه مهاجمین از کانال‌های پنهانی برای اهداف مخرب خود استفاده می‌کنند که داده را درون برنامه‌های شناخته شده‌ای

مانند شبکه‌های اجتماعی قرار می‌دهد. شبکه‌های اجتماعی از نام‌های دامنه مشخصی استفاده می‌کنند که در نتیجه مهاجمین با سوءاستفاده از این امکان، ترافیک مخرب خود را در ترافیک عادی موجود قرار می‌دهند و شناسایی را دشوارتر می‌کنند.

رمزنگاری برای محرمانگی پیام‌ها کاربرد فراوانی دارد. در رمزنگاری هدف ناخوانا کردن پیام‌های محرمانه است، بنابراین مانع از این می‌شود که شخص سومی از محتوا پیام محرمانه آگاهی پیدا کند اما ناظران بیرونی ممکن است از وجود این پیام‌ها اطلاع پیدا کنند. اطلاع از وجود ارتباطات بین دو نفر برای یک برنامه ممکن است عواقب جبران‌ناپذیری را در پی داشته باشد به همین دلیل این برنامه‌ها باید از کانال پنهان استفاده کرده تا هیچ‌گونه نشانه‌ای از برقراری ارتباطات دیده نشود[۱۴]کانال پنهان سازوکاری برای انتقال اطلاعات بین موجودیت‌هایی است که بنا به خط‌مشی‌های امنیتی مجاز به ارتباط با یکدیگر نیستند. [۱۵]

هر منبع اشتراکی به صورت بالقوه این قابلیت را دارد که به عنوان یک کانال پنهان مورد استفاده قرار گیرد. برای پیاده‌سازی کانال‌های فرمان و کنترل پنهان می‌توان از پروتکل‌های شبکه مانند آی‌پی، تی‌سی‌پی، دی‌ان‌اس و غیره استفاده کرد [۱۶]. در اغلب موارد، کانال‌های پنهان از ویژگی‌های برنامه‌ریزی نشده این پروتکل‌های شبکه استفاده کرده تا اطلاعات خود را ذخیره کنند. تعداد زیاد پروتکل‌های شبکه و پیچیدگی آن‌ها این امکان را فراهم می‌کند که تقریباً تعداد نامحدودی کانال پنهان داشته باشیم .

بات‌نت‌ها را می‌توان براساس دو معیار مرتبط با کانال‌های فرمان و کنترل طبقه‌بندی نمود: ساختار و پروتکل. بات‌نت‌ها براساس ساختار کانال‌های فرمان و کنترل خود به دو دسته متمرکز و غیرمتمرکز و براساس پروتکل مورد استفاده در کانال‌های فرمان و کنترل به سه نوع مبتنی بر اچ‌تی‌تی‌پی، مبتنی بر آی‌آرسی و نظیر به نظیر تقسیم می‌شوند. مدیران بات‌نت در ابتدا از سرویس‌دهنده آی‌آرسی برای کنترل بات‌نت‌های خود استفاده کردند. به دلیل اینکه سرویس‌دهنده آی‌آرسی یک نک نقطه شکست برای بات‌نت است با تشخیص آن، بات‌نت به راحتی منحل می‌شود. در نتیجه مهاجمین سعی کردند تا از روش بهتری برای کنترل بات‌های خود استفاده کنند .

استفاده از پروتکل اچ‌تی‌تی‌پی به عنوان کانال فرمان و کنترل امروزه رواج دارد چون یکی از مزیت‌های این نوع بات‌نت مخفی ماندن ترافیک کانال فرمان و کنترل در میان ترافیک اچ‌تی‌تی‌پی معمول مرور کاربران از صفحات وب است. در یک بات‌نت مبتنی بر اچ‌تی‌تی‌پی، ابتدا مدیر بات یک سرویس‌دهنده وب برپا کرده و فرامین خود را در آن قرار می‌دهد. سپس بات‌ها به طور دوره‌ای به این سرویس‌دهنده متصل‌شده تا جدیدترین فرامین را دریافت کنند. با این‌حال مکان‌یابی سرویس‌دهنده فرمان و کنترل هنوز یک مشکل رایج برای این نوع بات‌نت است. برای مثال اگر بات‌ها از آدرس‌های دامنه ثابتی که درون کد آن‌ها قرار دارد برای دسترسی به این سرویس‌دهنده استفاده کنند، با احتمال بالایی شناسایی خواهند شد .

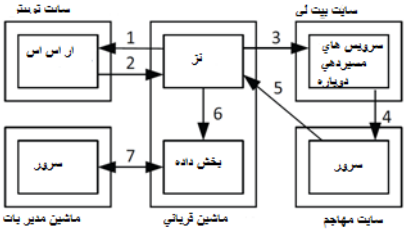
برای حل این مشکل، مهاجمین به الگوریتم‌های تولید دی‌ان‌اس روی آوردند. از آن‌جایی‌که سرویس دی‌ان‌اس یکی از مهم‌ترین سرویس‌ها در شبکه اینترنت است، چندان عجیب نیست که مهاجمین از آن جهت مقاوسازی بات‌نت خود استفاده کنند. مهاجمین از سرویس دی‌ان‌اس بهره می‌برند تا سرویس‌دهنده‌های فرمان و کنترل بات‌نت خود را پنهان کنند. تغییر پی‌درپی نام دامنه [۱۷] و تغییر پی‌درپی آدرس آی‌پی[۱۸] دو تکنیکی است که مهاجمین با استفاده از سرویس دی‌ان‌اس پیاده‌سازی می‌کنند. این تکنیک‌ها به مهاجم کمک می‌کنند تا سرویس‌دهنده‌های فرمان و کنترل خود را به صورت دوره‌ای و پویا تغییر داده و از قرار گرفتن آدرس‌های آن‌ها در فهرست‌های سیاه جلوگیری کنند. با این که شناسایی بات‌نت‌هایی که از این روش استفاده می‌کنند مشکل‌تر شده است ولی هنوز غیرممکن نیست .روش انعطاف‌پذیرتر دیگری که بات‌نت‌ها از آن برای کانال فرمان و کنترل خود استفاده می‌کنند، استفاده از پروتکل‌های شبکه نظیربه‌نظیر است. استفاده از این طراحی بات‌نت را به طور کامل غیرمتمرکز کرده و شناسایی و ردیابی آن را مشکل‌تر خواهد کرد .

در سال‌های اخیر تحقیقات زیادی درباره توسعه بات‌نت‌های نسل جدید با انواع مختلفی از کانال‌های فرمان و کنترل پنهان انجام شده است. در این پژوهش سعی شده است مهم‌ترین روش‌های کانال‌های پنهان پیشنهاد شده به منظور استفاده در کانال فرمان و کنترل بات‌نت‌ها شرح داده شود.

شبکه‌های اجتماعی امکان دست‌یابی به شکل جدیدی از برقراری ارتباط و به اشتراک‌گذاری محتوی در اینترنت را فراهم آورده‌اند. این شبکه‌ها دارای ویژگی‌های ذاتی از قبیل توزیع‌شدگی، به اشتراک‌گذاری آسان اطلاعات و غیره هستند که آن‌ها را به رسانه‌ای ایده‌ال جهت سوءاستفاده توسط مدیران باتنت تبدیل کرده است. این خصوصیات به مهاجمین این فرصت را می‌دهد تا با نصب و اجرای باتنت، جمعیت انبوهی از کاربران را اداره و تحت نفوذ خود قرار دهند و آنان را مجبور کنند تا برعلیه سایر کاربران اینترنت اقدام کنند حتی بدون این‌که خودشان از این موضوع اگاهی داشته باشند [۱۹].

انواع مختلف باتنت‌های مبتنی بر شبکه‌های اجتماعی ارائه شده است که در زیر با تعدادی از آن‌ها و عملکردشان آشنا خواهیم شد.

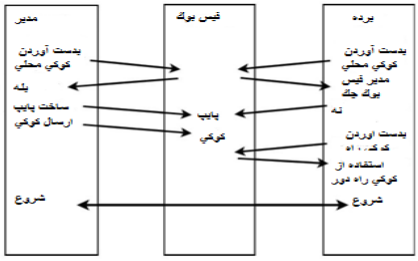
-بات نت نز: این نوع باتنت در سال ۲۰۰۹ شناخته شد [۲۰] که از توییتر به عنوان کانال فرمان و کنترل استفاده می‌کند. باتنت نَز از حساب‌های کاربری بر روی توییتر استفاده می‌کند. مهاجم حساب کاربری خود را فعال و به‌روزرسانی می‌کند تا بدین وسیله بات‌های خود را کنترل کند. بات‌ها هم به‌روزرسانی‌ها را از طریق آراس‌اس می‌خوانند و پیام‌ها را که با الگوریتم بیس۶۴ کدگذاری شده‌اند، کدگشایی می‌کنند. از نشانی‌هایی که به واسطه کدگشایی پیام ایجاد می‌شود، برای دانلود محتوای مخرب بر روی کامپیوتر آلوده استفاده می‌گردد. محتوای مخرب شامل فایل‌های gbpm.exe و gbpm.dll است. که اطلاعات و رمز عبور کاربران را سرقت می‌کند. شکل ۷ جریان حمله در باتنت نَز را نشان می‌دهد. بات درخواست اچ‌تی‌تی‌پی مربوط آراس‌اس نام‌کاربری را به سرور توییتر می‌دهد. توییتر در پاسخ به این درخواست آراس‌اس مربوطه را ارسال می‌کند که پیام‌های کدگذاری شده با بیس۶۴ را در خود دارد. بات پیام را کدگشایی کرده و یک یا چند نشانی را از آن استخراج می‌کند. توییتر محدودیت پیام ۱۴۰ کاراکتری دارد، به همین دلیل نشانی‌های طولانی بیش از ۱۴۰ کاراکتر را به نشانی‌های مختصر نگاشت و جایگزین می‌کند Bit.ly .چنین سرویسی را فراهم می‌کند و نگاشتی را بین نشانی‌های طولانی و نشانی‌های مختصر شده ای که خود تولید می‌کند، فراهم می‌آورد در واقع Bit.ly نام مختصری برای نشانی‌ها ایجاد می‌کند .بات با کلیک بر روی نشانی متعلق به Bit.ly، به سرور مهاجم هدایت می‌شود که فایل مخرب به صورت فشرده در آن‌جا قرار دارد. بات فایل را دانلود کرده و کدگشایی می‌کند و بعد از این‌که محتوای آن را از حالت فشرده خارج ساخت، آن را اجرا می‌کند. با اجرای محتوی، بات سعی در جمع‌آوری اطلاعات کاربر از روی میزبان آلوده می‌کند و اطلاعات به دست‌آمده را به سروری که مهاجم مشخص کرده، ارسال می‌کند.



شکل۷ جریان حمله در باتنت [۲۱]

-فیس‌کت [۲۲] :نوع دیگری از باتنت است که از دیوار مربوط به سایت اجتماعی فیسبوک به عنوان کانال فرمان و کنترل استفاده می‌کند. در طراحی این نوع باتنت، فرض بر آن شده که کاربران فیسبوک از این که در هر مرتبه بازدید از سایت، نام کاربری و رمز عبور خود را وارد کنند، ناراضی بوده و ترجیح می‌دهند که در هنگام وارد شدن به سایت، با صفحه کاربری خود روبه‌رو شوند. پس می‌توان نام کاربری و رمز عبور را در کوکی‌های سیستم پیدا کرد.براساس این فرض، باتنت با آلوده کردن سیستم قربانی، کوکی‌های فیسبوک را جست‌وجو کرده و در صورت پیدا کردن آن، کوکی‌ها را سرقت می‌کند و به این ترتیب می‌تواند به راحتی به حساب کاربری قربانی دسترسی پیدا کرده و به انجام فعالیت‌های مخرب خود بپردازد.همانطور که گفته شد، فیس‌کت از دیوار مربوط به کاربران فیسبوک استفاده می‌کند که به انتشار افکار و عقاید آنها اختصاص دارد. یکی

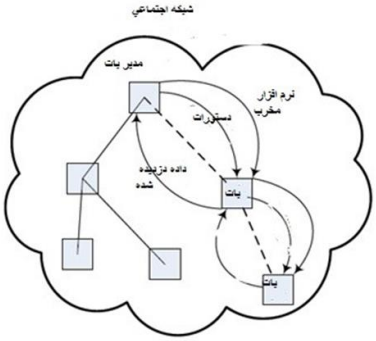
از مزیت‌های استفاده از دیوار این است که افراد می‌توانند روی دیوار دوست‌شان بنویسند یا روی مطالب آن ها نظرات و توضیحات خود را اضافه کنند. البته این به شرطی است که در تنظیمات حریم خصوصی به آنها اجازه داده شده باشد. بنابراین با توجه به توانایی دریافت اطلاعات از کاربرن مختلف، دیوار می‌تواند به عنوان یک کانال پنهان استفاده شود و بات‌ها می‌توانند پیام‌های خود را روی دیوار بنویسید یا از روی آن بخوانندشکل ۸ نمایی از جریان و رواند قرار دادن پیام در فیس‌کت می‌باشد:



شکل ۸ جریان حمله کانال فرمان و کنترل فیس‌کت[۲۲]

در معماری فیس‌کت از یک طرف مدیربات (M) را خواهیم داشت که مالک دیوار یا یکی از دوستان اوست که اجازه نوشتن روی دیوار را دارد. از طرف دیگر بات (S) را داریم که قربانی ما است. قربانی باید این اجازه را داشته باشد که روی دیوار بتواند اطلاعات به‌دست آورده شده را بنویسد. پس در اولین اقدام منتظر می‌ماند تا مدیربات کوکی کاربر را روی دیوار قرار دهد. زمانی که مدیربات شروع به اجرا کرد، کوکی مربوطه را روی دیوار می‌نویسد و بات سمت قربانی آن کوکی را از روی دیوار خود خوانده و از آن به بعد می‌تواند از آن استفاده کند و اطلاعات خود را برای مدیربات بفرستد. به همین ترتیب بات می‌تواند فرامین را از روی دیوار بخواند.

-استگوبات [۲۳]: در واقع یک بات‌نت با ساختار غیرمتمرکز است که در آن فرامین مدیر بات و داده‌های سرقتی توسط بات‌ها از طریق تصاویر اشتراکی شبکه اجتماعی فیسبوک منتقل می‌شوند. همان‌طورکه در شکل ۹ نشان داده شده، مدیر بات ابتدا میزبان‌های کاربرانی که با هم وابستگی اجتماعی دارند را آلوده می‌کند. هر بات، پروفایلی از فیسبوک را تحت کنترل دارد و فرامینی را که از سمت مدیربات برایش ارسال می‌شود را اجرا کرده و داده‌های سرقت شده را تحت پیام های پاسخ برای مدیربات ارسال می‌کند. استگوبات از تصاویری که توسط کاربران به اشتراک گذاشته می‌شود، به عنوان رسانه‌ای برای ساخت کانال فرمان و کنترل استفاده می‌کند. الگوریتم مسیریابی سیل‌آسا در طراحی این بات‌نت در نظر گرفته شده است.



شکل ۹ همبندی بات‌نت استگوبات [۲۳]

پنهان‌نگاری هنر برقراری ارتباط پنهانی است و هدف آن پنهان کردن ارتباط به وسیله قراردادن پیام در یک رسانه پوششی است به‌گونه ای که کم‌ترین تغییر قابل کشف را در آن ایجاد کند و نتوان موجودیت پیام پنهان در رسانه را حتی به صورت احتمالی آشکار ساخت. تفاوت اصلی رمزنگاری و پنهان‌نگاری آن است که در رمزنگاری، هدف اختفا محتویات پیام و نه به طور کلّی وجود پیام، اما در پنهان‌نگاری هدف مخفی کردن هر گونه نشانه ای از وجود پیام است. در مواردی که تبادل

اطلاعات رمزشده شکل آفرین است باید وجود ارتباط پنهان گردد. به عنوان مثال، اگر شخصی به متن رمزنگاری شده‌ای دسترسی پیدا کند، به هر حال متوجه می‌شود که این متن حاوی پیام رمزشده می‌باشد. اما در پنهان‌نگاری شخص سوم ابتدا از وجود پیام مخفی در متن اطلاعی حاصل نمی‌کند. حتی در موارد حساس ابتدا متن را رمزنگاری کرده، آنگاه آن را در متن دیگری پنهان نگاری می‌کنند.

انتشار اولین مرحله در ایجاد باتنت استقرار بدافزار و آلوده‌سازی میزبان‌های شبکه به کد مخرب بات است. بدافزار برنامه اجرایی است که میزبان‌های کاربران را آلوده کرده و برنامه‌های مورد نیاز برای ایجاد باتنت را بر روی میزبان قرار می‌دهد. استگوبات به گونه‌ای طراحی شده است تا کاربرانی که از طریق وابستگی‌های اجتماعی در شبکه اجتماعی فیسبوک به هم متصل شده‌اند را آلوده کند. در واقع، کد مخرب بات از طریق حملات بدافزاری به شبکه‌های اجتماعی]۲۴[انتشار پیدا می‌کند.برای مثال، فرض کنید در یک شبکه اجتماعی امکان مبادله نامه‌های الکترونیکی بین کاربران مختلف وجود دارد. مهاجم با ارسال نامه‌های الکترونیکی حاوی کد مخرب بات، میزبان‌های تعدادی از کاربران این شبکه اجتماعی را آلوده می‌کند.

در استگوبات ، هر بات دارای لیست برنامه‌ها و حملات از پیش تعریف شده‌ای است از قبیل سرقت آدرس‌های پست الکترونیکی و رمز عبور قربانی، اطلاعات کارت اعتباری و غیره. هم‌چنین در طراحی‌های پیشرفته‌تر این باتنت، هر بات دستوراتی را انجام می‌دهد که از سمت مدیر بات ارسال می‌شوند. برای مثال، بات‌ها دستوری را مبنی بر جستجو واژه‌های کلیدی از سمت مدیر بات دریافت می‌کنند و جستجوهای خود را در غالب پاسخ برای مدیر بات ارسال می‌کنند.

استگوبات از دو نوع ساختار پیام در شبکه استفاده می‌کند. ابتدا پیام‌های دستوری که توسط مدیر بات به صورت همه‌پخشی در شبکه ارسال می‌شود و پیام‌های پاسخ که در پاسخ به دستور مدیر بات از طرف بات‌های قرارگرفته بر روی میزبان‌های آلوده ارسال می‌شوند. پیام‌های پاسخ می‌توانند شامل پیام‌هایی باشند که به صورت محلی تولید شده یا پیام‌هایی باشند که توسط بات‌ها در طی مسیر انتقال داده می‌شوند تا به مدیر بات برسد.[۲۴]

-فیس بات: در [۱۹]با سوءاستفاده از امکانات شبکه اجتماعی فیسبوک و با استفاده از مفهوم پاپت‌نت‌ها [۲۶] باتنت جدیدی با نام فیس‌بات را طراحی کرده‌اند .عناصر قرار گرفته بر روی یک صفحه وب ممکن است از وب‌سایت‌های مختلفی گرفته شده باشند، به جای اینکه تمام آن‌ها در یک‌ها است قرار داشته باشند و به این ترتیب صفحه وب با استفاده از پیوندهایی آن‌ها را فراخوانی می‌کند. مهاجم به راحتی می‌تواند از این امکان سوءاستفاده کرده و صفحه مخربی را طراحی کند که شامل هزاران اتصال به سایت قربانی است. زمانی که یک کاربر عادی بدون اینکه متوجه باشد، این صفحه مخرب را بازدید می‌کند مرورگر عناصر قرار گرفته در سایت قربانی را دانلود کرده و با این روش پهنای باند وی را مصرف می‌کند. به این ترتیب حملات پاپت‌نت به صورت توزیع‌شده شکل می‌گیرد. استفاده از جاوا اسکریپت امکان راه‌اندازی حملات انعطاف‌پذیرتر و قدرتمندتری را فراهم می‌کند به طوری‌که کاربران می‌توانند مکرراً از سایت قربانی عناصر را دانلود کرده و یا انواع حملات مانند پویش درگاه و حملات محاسباتی را می‌تواند انجام دهند. قدرت این حملات به سه عامل بستگی دارد:

- شهرت صفحه مخرب: هرچه شهرت صفحه مخرب بالا باشد و کاربران زیادی آن را بازدید کرده و حمله قدرتمندتری انجام می‌گیرد .
- مدت زمان بازدید از صفحه مخرب: هرچقدر مدت زمان بازدید بیش‌تر باشد، حمله قدرتمندتری شکل می‌گیرد.
- پهنای باند کاربران عادی که صفحه مخرب را بازدید می‌کنند و تأخیر آن‌ها نسبت به سایت قربانی: این عوامل تعداد دانلودها را در هر ثانیه تعیین می‌کند[۲۵]

برای ایجاد این باتنت، مهاجم با استفاده از قابلیت برنامه‌کاربردی فیسبوک برنامه با نام "تصویر روز " ایجاد کرده که در هر روز تصاویر مختلفی را از نشنال ژئوگرافی برای کاربران فیسبوک نمایش می‌دهد. کاربران با اضافه کردن برنامه تصویر روز به صفحه کاربری خود، در هر بار کلیک بر روی این برنامه باعث حمله جلوگیری از سرویس توزیعی بر روی سرویس‌دهنده قربانی می‌شوند. مدیر بات کدی را درون برنامه قرار داده است که وقتی کاربر بر روی این برنامه کلیک می‌کند و تصویر را می‌بینند، درخواست‌های اچ‌تی‌تی‌پی برای میزبان قربانی تولید و ارسال می‌شود. به طور دقیق‌تر، برنامه چهار فریم پنهان را در

ازای تصاویر درون برنامه‌ای که بر روی سایت قربانی قرار گرفته، تعبیه می‌کند. هر زمان که کاربر بر روی برنامه کلیک می‌کند، تصاویر درون برنامه‌ای از سایت قربانی فراخوانی و واکشی می‌شود که در نتیجه یک درخواست ۶۰۰ کیلو بایت برای قربانی ارسال می‌شود. این درحالی است که کاربر شبکه اجتماعی به هیچ وجه از این اتفاقات آگاهی پیدا نکرده و این تصویر هرگز برای او نمایش داده نمی‌شود. شکل ۱۰ نمونه‌ای از کد درج در برنامه را نشان می‌دهد که باعث می‌شود تصویری با نام "image1.jpg"از سایت قربانی با نام victim-host واکشی گردد و درون یک فریم مخفی از برنامه تصویر روز قرار گیرد. [۲۶]

```
<iframe name="1" style="border: 0px none #ffffff;
width: 0px; height: 0px;"
src="http://victim-host/image1.jpg?
fb_sig_in_iframe=1&amp;
fb_sig_time=1202207816.5644&amp;
fb_sig_added=1&amp;
fb_sig_user=724370938&amp;
fb_sig_profile_update_time=1199641675&amp;
fb_sig_session_key=520dabc760f374248b&amp;
fb_sig_expires=0&amp;
fb_sig_api_key=488b6da516f28bab8a5ecc558b484cd1&amp;
fb_sig=a45628e9ad73c1212aab31eed9db500a">
</iframe><br/>
```

شکل ۱۰ یک فریم پنهان قرار گرفته در کد برنامه [۱۹]

- بات اجتماعی: در حقیقت نرم‌افزار خودکاری است که حساب‌های کاربری مهاجم و یا حساب‌های کاربری دزدیده شده توسط او را کنترل می‌نماید. این بات‌های اجتماعی توانایی فعالیت‌های مهمی از قبیل ارسال پیام و درخواست دوستی را دارند. تفاوت بات‌های اجتماعی با بات‌های خود اعلان (بات‌هایی هستند که توییتر[۱] از آنها برای به‌روزرسانی پیش‌بینی وضع هوا استفاده می‌نماید) و بات‌های هرزه (بات‌هایی هستند که پیام‌های[۲] ناخوانسته را درحجم وسیع برای کاربرانی ارسال می‌کند که راضی به دریافت آنها نیستند) در این است که بات‌های اجتماعی برای القای خود به عنوان یک هویت انسانی طراحی شده‌اند. بات‌های اجتماعی برای رسیدن به این هدف خود یا باید رفتارهای انسان تقلید نمایند یا با استفاده ازهوش مصنوعی مانند یک کاربر انسانی شبیه‌سازی شوند. بنابراین بات اجتماعی برای نفوذ در یک شبکه‌ی اجتماعی استفاده می‌شود که هدف از آن نفوذ بدست آوردن جایگاهی است که بتواند گراف اجتماعی (همان ساختار اجتماعی) یک شبکه اجتماعی را توسط برقراری ارتباط با طیف وسیعی از کاربران آن به خطر بیاندازند.بات اجتماعی با مقیاس بالا در شبکه‌های اجتماعی نفوذ می‌کنند و این از پیامدهای جدی امنیتی در این زمینه است. بات اجتماعی یک شبکه اجتماعی را توسط بسیاری روابط غیرواقعی که با کاربران ایجاد می‌نماید، آلوده می‌کند، به این معنی که دیگر نمی‌توان به این شبکه اجتماعی اعتماد کرد.

به عنوان دومین نکته می‌توان گفت، هنگامی که بات اجتماعی درون یک شبکه اجتماعی نفوذ می‌کند، به راحتی می‌تواند با بهره‌گیری از این جایگاه به نشر اکاذب اقدام نماید و نظر جمعی و عمومی کاربران را نسبت به موضوع خاصی تغییردهد و یا در موارد شدیدتر با توجه به این‌که داد و ستدهای الگوریتمیک معمولاً از نظرات استخراج شده از شبکه‌های اجتماعی برای حدس و پیش‌بینی بازار سهام استفاده می‌نمایند، بات‌های اجتماعی به راحتی می‌توانند آن‌ها را تحت تأثیر قرار دهند.

به عنوان آخرین نکته، وقتی یک بات اجتماعی در شبکه‌ی اجتماعی نفوذ کرد ممکن است اقدام به جمع‌آوری اطلاعات خصوصی یک کاربر مانند ایمیل، شماره تلفن و دیگر اطلاعات شخصی که ارزش مالی دارند، نماید. برای یک مهاجم، این اطلاعات به‌دست آمده ممکن است در ایجاد یک پروفایل جدید بکار رود و با ایجاد این پروفایل جدید قادر به حملاتی همچون ارسال هرزه‌نامه در مقیاس بالا و تور اندازی و غیره است.شبکه بات‌نت اجتماعی در واقع مجموعه‌ای از بات‌های اجتماعی است که توسط یک کنترل‌کننده انسانی به نام مدیر بات کنترل و نگهداری می‌شود. [۲۷]

[۱] Self-declared bot

[۲] Spambot

۴.کانال کنترل و فرمان

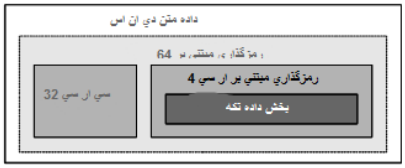
همانطور که گفته شد کانال فرمان راه ارتباطی بین مدیر بات و اعضای بات است در ادامه کانال های کنترل و فرمان توضیح داده خواهد شد:

-دی‌ان‌اس به عنوان کانال فرمان و کنترل پنهان: دی‌ان‌اس ویژگی‌هایی دارد که می‌تواند در مقایسه با سایر پروتکل‌های لایه کاربرد انتخاب خوبی برای کانال فرمان و کنترل بات‌نت باشد. مهم‌ترین مزیت استفاده از دی‌ان‌اس این است که حتی در شبکه‌های تحت نظارت شدید فایروال‌ها و پروکسی‌ها، دی‌ان‌اس به راحتی و بدون هیچ اقدامی می‌تواند از این نظارت‌ها عبور کند. این درحالی است که روش‌های متعددی برای بررسی و تحلیل ترافیک‌های مبتنی بر پروتکل‌های دیگر مانند اچ‌تی‌تی‌پی وجود دارد. از طرفی این پروتکل به صورت یک سیستم توزیعی طراحی شده که باعث ایجاد انعطاف‌پذیری بالا در آن می‌شود. برای قرار دادن اطلاعات درون ترافیک دی‌ان‌اس می‌توان از پروتکل دی‌ان‌اس و از رکوردهای آن استفاده کرد. هر نوعی از رکوردهای دی‌ان‌اس این قابلیت را دارد که به عنوان کانال فرمان و کنترل در بات‌نت استفاده شود و سرعت ارتباطات، بسته به میزان داده‌ای دارد که درون هر رکورد از هر نوع قرار می‌گیرد. رکوردهای تی‌اکس‌تی می‌توانند بیش‌ترین داده را در خود ذخیره کنند. فیدربات و مورتو دو بات‌نتی هستند [۲۸] که از رکورد تی‌اکس‌تی در پیام‌های دی‌ان‌اس به عنوان ترافیک کانال فرمان و کنترل خود استفاده می‌کند. در ادامه به نحوه عملکرد فیدربات خواهیم پرداخت .

در [۲۹] تحقیقات خود با استفاده از تحلیل مهندسی معکوس از وجود بات‌نتی با نام فیدربات خبر دادند که از پیام‌های دی‌ان‌اس به عنوان یک حامل برای ترافیک کانال فرمان و کنترل خود استفاده می‌کند. فیدربات از پیام‌های دی‌ان‌اس با رکوردهای تی‌اکس‌تی برای ارتباط با مدیر بات استفاده می‌کند. این نوع رکورد ارزش عملیاتی ندارد و اغلب توضیحاتی را در مورد صاحب این نام دامنه و هویت آن ارائه می‌کند. علاوه براین نام دامنه درخواستی برای ارسال پارامترهای معینی مانند پارامترهای اشتقاق کلید از بات به سرور فرمان و کنترل استفاده می‌شود.

فیدربات تحلیل‌گر دی‌ان‌اس قرار گرفته بر روی میزبان آلوده را دور زده و به طور مستقیم درخواست خود را به سرور فرمان و کنترل ارسال می‌کند. دراین‌صورت هیچ ردی از ارتباطات مربوط به کانال فرمان و کنترل در گزارشات تحلیل‌گر دی‌ان‌اس و حافظه نهان باقی نمی‌ماند.ترافیک فرمان و کنترل در فیدربات به تعدادی قطعه تقسیم می‌شود که ماکزیمم اندازه هر قطعه ۲۲۰ بایت است. هر قطعه در بخش آر-دیتا پاسخ دی‌ان‌اس از رکورد تی‌اکس‌تی ارسال می‌شود که با استفاده از بیس ۶۴ کدگذاری شده است. در زیر نمونه‌ای از پیام ارسال شده دیده می‌شود.[۳۵]

برای اینکه پیام‌ها شناسایی نشوند، قسمت بیشتر پیام با استفاده از آرس۴ رمزگذاری می‌شود. فیدربات از کلیدهای رمزگذاری متنوعی استفاده می‌کند. همان‌طور که قبلاً هم گفته شد، بخش مشخصی از نام دامنه درخواستی دی‌ان‌اس، برای ارسال پارامترهای اشتقاق کلید استفاده می‌شود. برای مثال، یکی از توابع اشتقاق کلید به عنوان ورودی زیر رشته qdparam را از نام دامنه درخواستی دریافت کرده وسپس با استفاده از آرس۴ با رشته "feedme" رمز می‌کند و در نهایت کلیدی که از این کار حاصل می‌شود برای رمزگشایی قطعات پیام ارسال شده، استفاده می‌شود. درصورتی‌که یکی از قطعه‌ها در بین راه گم شود، رمزگشایی سایر قطعات انجام نخواهد شد. علاوه براین از کدهای افزونگی چرخشی برای قطعات پیام استفاده می‌کنند تا از صحت نتایج رمزگشایی اطمینان حاصل شود. شکل ۱۱ ساختار قطعات پیام در فیدربات را نشان می‌دهد



شکل ۱۱ ساختار قطعات پیام در فیدربات[۳۰]

- اسکایپ به عنوان کانال فرمان و کنترل پنهان:اسکایپ یکی از پرکاربردترین برنامه‌های کاربردی نظیر به نظیر بر روی اینترنت است که خدماتی از قبیل تماس از طریق وُیپ ، پیام‌رسانی فوری ، اس‌ام‌اس و غیره را با هزینه کم برای میلیون‌ها کاربر فراهم می‌آورد. از آنجایی‌که اسکایپ یک برنامه منبع باز نیست با این حال با استفاده از قابلیت واسط برنامه‌نویس کاربر این امکان را برای توسعه‌دهندگان فراهم می‌آورد تا با ایجاد افزونه‌های سفارشی بر روی شبکه اسکایپ به تعامل و ارتباط بپردازند و می‌توانند از قابلیت اطمینان اسکایپ استفاده کرده و به راحتی فایروال‌ها را دور بزنند. از طرفی پروتکل مورد استفاده توسط اسکایپ ثبت نشده، بنابراین تحلیل و مهندسی معکوس ترافیک حاصل از آن بسیار دشوار است .

اسکایپ با رمز کردن تمامی ارتباطات خود محرمانگی کاربران را حفظ کرده و همچنین با ایجاد یک زیرساخت ارتباطی غیرمتمرکز تحمل‌پذیری نسبت به خطا را نیز بالا می‌برد. در نتیجه به زودی مهاجمین متوجه خواهند شد که ارتباطات رمزگذاری شده اسکایپ می‌تواند به راحتی محرمانگی فعالیت‌های غیرقانونی آن‌ها را حفظ کرده و حتی بدتر از آن زیرساخت اسکایپ می‌تواند تمامی شرایط مطلوب را برای ایجاد یک بات‌نت با ویژگی‌های انعطاف‌پذیری، مقرون به صرفه بودن، استقرار آسان و اختفا را فراهم کند. ویژگی‌هایی جالب و مطلوب اسکایپ به عنوان کانال فرمان و کنترل بات‌نت عبارتند از:

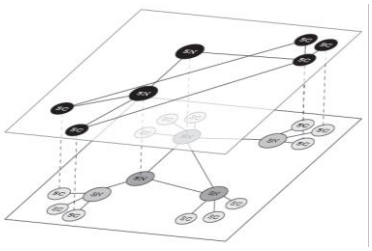
- جدا کردن ترافیک بات از ترافیک عادی شبکه دشوار است.
- با به کارگیری یک شبکه غیرساخت‌یافته، شبکه مخرب ایجاد شده هیچگونه نقطه شکست یا تگنا ارتباطی ندارد. به عبارت دیگر هیچ تفاوتی از نظر سلسله مراتبی میان گره‌های آن وجود ندارد .
- عدم ساختار سلسله مراتبی این امکان را می‌دهد که از هر گره تحت کنترل به عنوان یک نقطه ورود برای مدیر بات استفاده شود.
- شبکه پوششی ایجاد شده نسبت به فقدان و نبود بات‌ها تحمل‌پذیری دارد به این معنا که هر نود (یا بات) تنها از مجموعه کوچکی از همسایه‌های خود اطلاعات دارد که برای انتقال پیام مورد استفاده قرار می‌گیرد و هیچ اطلاعاتی را از مدیر بات شامل نمی‌شود .
- وجود استراتژی‌های مسیریابی شفاف و پویا که وظیفه مسیریابی پیام‌ها از طریق مسیرهای جایگزین را دارند، حتی زمانی که یک یا چندین بات در دسترس نباشند. (برای مثال ممکن است غیرفعال شده باشند)[۳۵]

در[۳۰] مدل مفهومی از یک بات‌نت ارائه شده است که در آن از زیرساختی همچون اسکایپ سوء استفاده کرده و با استفاده از یک زیرساخت پوششی بر روی آن، ردیابی مدیربات را با مشکل مواجه می‌کند و یا برای از بین بردن بات‌نت، عملکرد کاربران قانونی را با مشکل مواجه می‌کند. آزمایشات انجام شده نشان می‌دهد که وجود این بات‌نت عملی است و انعطاف‌پذیری بالایی را تضمین می‌کند و اطمینان می‌دهد تا درصورتی‌که تعداد زیادی از بات‌ها آفلاین باشند، پیام‌ها انتقال پیدا کنند .

اسکایپ امنیت بالایی دارد. از طرف دیگر نرم‌افزاری که امنیت بالایی دارد و از سیاست‌های حریم خصوصی پشتیبانی می‌کند، حس مثبتی از اعتماد را در میان کاربران خود ایجاد کرده و افراد بیش‌تری را به جذب خود می‌کنند تا با نصب برنامه از خدمات آن‌ها استفاده کنند. وجود نقطه ضعف در معماری نرم‌افزار به مهاجمین این امکان را می‌دهد که از این ویژگی‌ها برای اهداف مخرب خود استفاده کنند. در واقع آن‌ها از واسط برنامه‌نویسی کاربر این نرم‌افزار سوءاستفاده کرده تا بدافزار خود را مستقر کنند. این کرم‌ها به عنوان افزونه‌های اسکایپ استقرار پیدا می‌کنند. زمانی که افزونه پیامی را صادر می‌کند (برای مثال فرستادن پیام یا ایجاد یک گفتگو)، اسکایپ دقیقاً طوری رفتار می‌کند که این دستور از طرف یک کاربر قانونی ارسال شده است. برای مثال تمامی ترافیکی که از افزونه‌های یک میزبان خارج می‌شود به‌صورت خودکار رمز شده و بدافزار از این ویژگی برای پنهان کردن خود و فعالیت‌هایش استفاده می‌کند. تمام این ویژگی‌ها باعث می‌شود که واسط برنامه‌نویسی کاربر برای مهاجمینی که به دنبال یک ابزار قدرتمند و جدید برای کنترل بات‌نت خود هستند، ایده‌ای جذاب و محرک باشد.

واسط برنامه‌نویسی کاربر در اسکایپ به توسعه‌دهندگان این امکان را می‌دهد تا برنامه‌های کاربردی خود را با استفاده از ویژگی‌هایی همچون ارسال پیام‌های چت یا اس‌ام‌اس، شروع و یا هدایت تماس‌ها، جستجو دوستان و غیره ایجاد کنند.

متأسفانه امنیت واسط برنامه‌نویسی کاربر مانند امنیت خود برنامه اسکایپ نیست. نقطه ضعف واسط برنامه‌نویسی کاربر این است که هیچ کنترلی بر روی تعداد پیام‌هایی ارسالی توسط افزونه ندارد. به طور کلی، تمام فعالیت‌های ممکنی که یک کاربر قانونی می‌تواند از طریق یک سرویس‌گیرنده انجام دهد، می تواند به صورت خودکار توسط افزونه انجام شده بدون اینکه هیچ‌گونه نظارتی بر روی پیام‌های هرزه صورت گیرد. شکل ۱۲نشان می‌دهد که چگونه بات‌ها در این شبکه باهم ارتباط برقرار می‌کنند. در این شکل بات‌ها به رنگ سیاه و در لایه بالایی قرار گرفته اند که از طریق خط تیره به کاربران آلوده در شبکه اسکایپ متصل شده‌اند. بات‌ها پیام‌های خود را به طور مستقیم برای یکدیگر ارسال می‌کنند بدون اینکه از نحوه مسیریابی در شبکه اسکایپ زیربنایی اطلاع داشته باشند. طراحی شبکه اسکایپ به صورت یک شبکه نظیر به نظیر ترکیبی با سرویس‌دهنده‌های مرکزی، ابر گره‌ها ، سرویس‌گیرنده‌های عادی است. ابر گره‌ها نقش مهمی را در کل شبکه بازی می‌کنند. مجموعه این گره‌ها مسئول راه‌اندازی شبکه هستند و به عنوان نقطه ورود در زیرساخت شبکه عمل می‌کنند و پیامی که برای یک گره ارسال می‌شود، از طریق این گره‌ها مسیریابی می‌گردد.



شکل ۱۲ شبکه بات‌نت بر روی شبکه اسکایپ [۳۰]

از آن جایی که تمامی پیام‌ها با استفاده از سرویس‌گیرنده‌ها از طریق ابر گره‌ها مسیریابی می‌شود، شبکه پوششی بات‌نت روی آن، هیچ‌گونه سلسله مراتبی را بین سرویس‌گیرنده‌ها و ابر گره‌ها قائل نمی‌شود.

-شبکه تور به عنوان کانال کنترل و فرمان: شبکه تور سرویس برخطی است که به کاربران این امکان را می‌دهد تا به صورت ناشناس از صفحات وب بازدید کنند. اخیراً محققان بات‌نت‌هایی با نام اسکای‌نت [۳۱] و مِوید [۳۲]را شناسایی کردند که توسط مهاجم از طریق سرور آی‌آرسی که داخل شبکه تور قرار دارد، کنترل می‌شوند. در نتیجه به دلیل این‌که یافتن مکان واقعی این سرور دشوار است، غیرفعال کردن این نوع بات‌نت به راحتی امکان‌پذیر نمی‌باشد. از طرفی ترافیک کانال فرمان و کنترل بات‌نت توسط شبکه تور رمزگذاری شده و نمی‌تواند توسط سیستم‌های تشخیص نفوذ شناسایی شود. پروتکل‌های این سرویس مخفی به کاربران این امکان را می‌دهد تا انواع مختلفی از سرویس‌ها از قبیل وب‌سایت‌ها، سرورهای پیام فوری، را اجرا کنند [۳۳].سرویس‌های مخفی یکی از قابلیت‌های شبکه تور است و این امکان را فراهم می‌کند تا سرویس‌های مخفی و ناشناسی را ایجاد کرده که تنها از طریق تور قابل دسترس هستند. وجود این سرویس‌دهنده‌های مخفی در تور با استفاده از کلید رمزگذاری عمومی اعلان می‌شود که در سرویس‌دهنده‌های فهرست تور نمایه می‌شوند. علاوه بر کلیدهای تولید شده برای این سرویس‌ها، یک شبه دامنه با پسوند onion. تولید می‌شود که برای تحلیل و ارتباط با سرور پنهان در تور استفاده می‌شود. این خدمات تنها می‌توانند از درون شبکه‌ی تور از طریق این نام دامنه‌ی قابل دسترسی باشند. در نتیجه نه تنها از هیچ طریقی آدرس آی‌پی سرویس‌دهنده پنهان آشکار نخواهد شد، بلکه سرویس‌دهنده‌های فهرست هم نمی‌توانند هویت آن‌چه را که در پس این دامنه است، شناسایی کنند .اسکای‌نت سرویس‌دهنده‌های فرمان و کنترل خود را به عنوان سرویس‌دهنده‌های پنهان در تور قرار می‌دهد و تمامی میزبان‌های آلوده طوری تنظیم خواهند شد که بخشی از شبکه تور باشند.

مزایای استفاده از این دیدگاه برای بات‌نت:

- ترافیک بات‌نت رمزگذاری خواهد شد که کمک می‌کند تا از ناظران شبکه در امان بماند .

- قرار گرفتن سرویس‌دهنده‌های فرمان و کنترل در شبکه تور باعث می‌شود که منشاء، مکان، هویت آن‌ها مخفی مانده و طول عمر بات‌نت را افزایش خواهد داد.
- سرویس‌های پنهان یک شبه دامنه سطح بالا با پسوند onion. تولید می‌کند که در معرض بررسی ترافیک قرار نمی‌گیرد .
- مدیر بات به آسانی می‌تواند با تولید کلید خصوصی برای سرویس پنهان، سرویس‌دهنده‌های فرمان و کنترل خود را جابه‌جا کنند .

تعدادی از شبه دامنه‌های onion. را که درون بات تعبیه شده در زیر نشان داده شده است که تعدادی از آن‌ها هنوز فعال هستند.همان‌طور که پیش از این گفته شد، بات‌نت یک سرویس مخفی تور بر روی میزبان آلوده بر روی پورت ۵۵۰۸۰ ایجاد می‌کند. به طور پیش فرض این پورت خالی است اما زمانی‌که مدیر بات دستور خاصی را بر روی سرور آی‌آرسی قرار می‌دهد، بات پراکسی را بر روی پورت ۵۵۰۸۰ باز خواهد کرد و سپس دستور از طریق یک دامنه onion. جدید قابل دسترس خواهد بود .بات‌نت اسکای‌نت می‌تواند برای راه‌اندازی حملات جلوگیری از سرویس توزیعی ، تولید بیت‌کوین‌ها ، استفاده از قدرت پردازش کارت گرافیک نصب شده بر روی میزبان قربانی، دانلود و اجرای فایل‌های دلخواه یا سرقت اعتبارنامه های ورودی از وب‌سایت‌ها از جمله حساب‌های کاربری بانکداری برخط مورد استفاده قرار بگیرد. بدافزار پشت صحنه‌ی این بات‌نت از طریق یوس‌نت منتشر می‌شود.درکل، می‌توان گفت که تور به خاطر طراحی و مکانیزم داخلی، یک پروتکل کامل برای بات‌نت‌ها به شمار می‌رود و تمامی ارتباطات مهم اسکای‌نت با سرورهای فرمان و کنترلش از طریق پروکسی مبادله می‌شود که به طور محلی بر روی میزبان آلوده در حال اجرا است.[۳۳]

۵. دسته‌بندی روش‌های تشخیص بات‌نت

تکنیک‌های بسیاری برای تشخیص بات‌نت‌ها یا شناسایی فعالیت‌های آن‌ها ارائه شده است. این تکنیک‌ها به طور کلی به دو روش مبتنی بر هانی‌نت و سیستم تشخیص نفوذ تقسیم می‌شوند.مطالعات اولیه در مورد بات‌نت‌ها بر اساس هانی‌نت‌ها بود. اکثر پژوهشگران برای تحلیل و رفتار بات‌ها هانی‌نت طراحی می‌کردند. اما هانی‌نت‌ها برای درک بهتر ویژگی و رفتارهای بات‌نت‌ها مناسب است و استفاده از این روش همیشه جوابگوی تشخیص بات‌نت‌ها نیست. به این دلیل پژوهشگران به بررسی و مطالعه روش‌های سیستم تشخیص نفوذ روی آوردند که این تکنیک‌ها در تشخیص بات‌نت‌ها کاراتر از روش‌های قبل هستند. به طور کلی، روش‌های تشخیص بات‌نت‌ها در سیستم تشخیص نفوذ می‌توانند به روش‌های مبتنی بر ناهنجاری۱ ، روش‌های مبتنی بر امضاء و روش‌های تشخیص ترکیبی تقسیم شوند[۳۴]. شکل ۳-۱۱ دسته‌بندی تکنیک‌های تشخیص بات‌نت‌ها نشان می‌دهد. براساس کارهای پیشین، ویژگی‌ها و خصوصیات هر کدام از تکنیک‌ها به شرح زیر است.

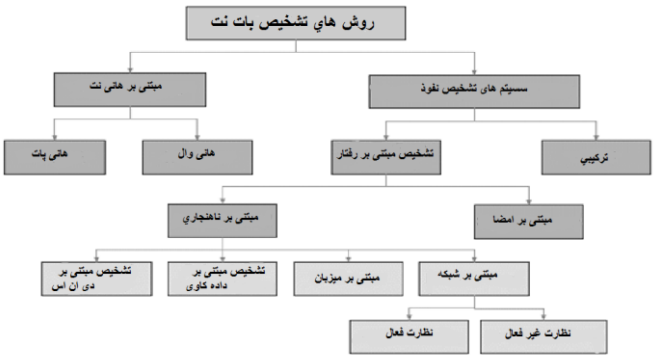
-روش تشخیص مبتنی بر هانی‌نت‌ها:هانی‌نت‌ها معمولاً برای جمع‌آوری اطلاعات از بات‌ها مناسب هستند. پس از جمع‌آوری اطلاعات این امکان را دارند که تکنولوژی استفاده شده در بات‌نت را تعیین کرده و یک آنالیز کاملی از ویژگی‌های بات‌نت اصلی ارائه دهند. معمولاً هانی‌نت‌ها برای شناسایی سرور کانال فرمان و کنترل توسط سیستم شناسایی مبتنی بر امضاء بات، به کار می‌روند. هانی‌نت‌ها برای شناسایی کارهای دودویی بات‌ها و نفوذ در بات‌نت‌ها هم استفاده می‌شوند. علاوه بر اینکه هانی‌نت‌ها برای درک تکنولوژی و خصوصیات بات‌نت به کار می‌روند، یکسری محدودیت‌هایی هم دارند که شامل:

- میزان محدودی از فعالیت‌های بهره‌برداری را می‌توانند ردیابی نمایند.
- عدم توانایی در قبضه کردن بات‌هایی که از شیوه‌های انتشار استفاده نمی‌کنند.

- فقط در مورد ماشین‌هایی که به تله آنها گرفتار شده‌اند، گزارش می‌دهند.

-سیستم تشخیص نفوذ:این سیستم‌ها معمولاً هم در شیوه‌های شناسایی مبتنی بر امضاء و هم در شیوه‌های شناسایی مبتنی بر ناهنجاری به کار می‌روند. شیوه‌های مبتنی بر امضاء معمولاً از الگوهای بات‌های جاری در سیستم تشخیص نفوذ استفاده می‌نمایند مانند اسنورت. ایده اصلی این است که اطلاعاتی در مورد ویژگی‌های بات‌نت از بسته‌های ترافیک مانیتور شده به دست آورد، آنها را به عنوان یک الگو امضاء زده در پایگاه دانش بات‌ها ثبت نماید. حال شناسایی بات‌نت با استفاده از این پایگاه دانش آسان است و فقط نیاز به یک مقایسه میان بایت‌های درون بسته‌ها با الگوهای درون پایگاه دانش داریم. اگر روش تشخیص مبتنی بر امضاء مزایای زیادی دارد ولی دارای معایبی هم هست که از جمله آنها می‌توان به این نکته اشاره نمود که این روش تنها توانایی شناسایی بات‌های شناخته شده که الگوهای آنها درون پایگاه دانش موجود است، را دارد و از شناسایی بات‌های ناشناخته عاجز است. عیب دیگر این روش این است که باید همواره سعی شود تا پایگاه دانش بروز باشد که این کار هزینه‌های مدیریتی زیادی را می‌طلبد و همین طور کارایی را هم کاهش می‌دهد. عیب دیگری که اوضاع را کمی وخیم‌تر می‌کند این است که این روش توانایی شناسایی با رقابتی که فقط اختلاف کمی با الگو دارند، را هم ندارد.[۳۵]

-روش تشخیص مبتنی بر ناهنجاری:تکنیک مبتنی بر ناهنجاری نوعی از روش تشخیص مبتنی بر رفتار است. این روش خود به روش‌های مبتنی بر دی‌ان‌اس ، مبتنی بر داده کاوی ، مبتنی بر میزبان و شبکه تقسیم‌بندی می‌شود. این تکنیک‌ها برای شناسایی بات‌نت‌ها از چندین روش ناهنجاری ترافیک شبکه از قبیل تاخیر زیاد شبکه، حجم بالای ترافیک، ترافیک بر روی درگاه‌های غیرمعمول و رفتار غیرعادی سیستم استفاده می‌کنند که می‌توانند نشان‌دهنده‌ی حضور بات‌های مخرب در شبکه باشند. بنابراین روش مبتنی بر ناهنجاری قادر به شناسایی بات‌نت‌های ناشناخته است. اما این روش نرخ هشدار نادرست بالایی را تولید می‌کند.



شکل ۱۳ تکنیک‌های شناسایی بات نت‌ها [۳۴]

- روش تشخیص مبتنی بر دی‌ان‌اس: تکنیک مبتنی بر دی‌ان‌اس، از طریق نظارت بر دی‌ان‌اس و ناهنجاری‌های ترافیک دی‌ان‌اس انجام می‌گیرد. برای استفاده از این تکنیک، باید بات‌نت‌ها ترافیک دی‌ان‌اس تولید کنند. معمولاً بات‌ها برای دسترسی به سروریس‌دهنده‌ها از پرس‌وجوی دی‌ان‌اس استفاده می‌کنند. این تکنیک برای پیداکردن مدیربات توسط بات‌ها روش مناسبی است زیرا بلافاصله بعد از تحلیل پرس‌وجوی دی‌ان‌اس موقعیت سرویس‌دهنده بات مورد نظر مشخص می‌شود.

- روش تشخیص مبتنی بر داده‌کاوی: روش‌های مبتنی بر داده‌کاوی بیش‌تر برای بهبود بخشیدن دقت تشخیص ارائه شده‌اند. روش تشخیص مبتنی بر داده‌کاوی یکی از تکنیک‌های موثر در تشخیص ترافیک فرمان و کنترل بات‌نت‌ها با استفاده از روش‌های یادگیری ماشین، دسته‌بندها و خوشه‌بندی به شمار می‌رود.

- روش تشخیص مبتنی بر میزبان: در تکنیک تشخیص مبتنی بر میزبان، ترافیک شبکه به منظور تشخیص سیستم‌های آلوده به بات نظارت و مانیتورینگ می‌شود. بات‌ها باعث تغییر فایل‌ها و رجیستری سیستم‌های آلوده می‌شوند. هم‌چنین بات‌نت‌ها یک سری از توابع کتابخانه‌ای و سیستمی را فراخوانی می‌کنند که از طریق این قابل شناسایی هستند.

- روش تشخیص مبتنی بر شبکه: در این تکنیک نظارت بر شبکه بیشتر بر روی دو مورد تمرکز دارد: ۱) تشخیص بات‌های انفرادی با استفاده از الگوهای ترافیک و یا محتوا، که می‌توانند سرویس‌دهنده فرمان و کنترل یا فعالیت‌های مخرب بات‌ها را افشا کنند. ۲) تحلیل ترافیک شبکه برای یافتن رفتارهای مشابه دو یا چند میزبان شبکه که دارای رفتارهای مخرب مانند بات‌ها دارند. نظارت و مانیتورینگ در تکنیک مبتنی بر شبکه می‌تواند به دو صورت فعال و غیرفعال انجام گیرد.

- روش تشخیص مبتنی بر امضاء :نیز مشابه دیگر روش‌های تشخیص بر اساس ناهنجاری از تحلیل رفتار شبکه استفاده می‌کند. این تکنیک دانشی را از قبل از طریق بات‌نت‌های شناخته شده یاد گرفته و براساس آن، می‌توانند فعالیت‌های بات‌ها را از ترافیک شبکه شناسایی کند. این روش دارای سرعت بالا در تشخیص است و نرخ هشدار نادرست پایین‌تری نسبت به سایر روش‌ها تولید می‌کند. اگرچه سیستم‌های مبتنی بر الگو دقیق‌تر هستند، اما مشکلاتی دارند که برخی از آن‌ها به ترتیب زیر است:اول این‌که، قادر به شناسایی بات‌های ناشناخته نیستند. دوم هر امضایی مربوط به یک بات مشخص است. در نتیجه اگر یک بات رفتار مختلفی داشته باشد در این حالت قابل تشخیص نیست؛ و سوم این‌که اگر تعداد بات‌ها مختلف باشند نرخ مثبت کاذب[۳]افزایش می‌یابد. در مقابل سیستم‌هایی که مبتنی بر ناهنجاری عمل می‌کنند تلاش دارند تا فعالیت‌های بات را با استفاده از مشاهده رفتارش شناسایی کنند. اگر این عمل به‌خوبی انجام شود، این دسته از سیستم‌ها قادرند به خوبی سیستم‌های مبتنی بر امضا در شناسایی بات‌ها دقیق باشند.

-روش تشخیص مبتنی بر ترکیبی:در تکنیک تشخیص بات‌نت مبتنی بر ترکیبی، دو یا چند سیستم‌های تشخیص نفوذ ترکیب می‌شوند. می‌توان روش‌های مبتنی بر دی‌ان‌اس را با روش‌های مبتنی بر ناهنجاری، روش‌های مبتنی بر امضاء را با روش‌های مبتنی بر ناهنجاری و یا روش‌های مبتنی بر داده‌کاوی را با روش‌های مبتنی بر ناهنجاری ترکیب نمود. به دلیل این که روش‌های مبتنی بر امضاء، دی‌ان‌اس و داده‌کاوی تنها قادر به شناسایی حملات شناخته شده هستند، بنابراین برای حل این مشکل باید با روش تشخیص مبتنی بر ناهنجاری که قادر به شناسایی حملات ناشناخته است، ترکیب شوند.

[۳] False positive

مراجع

T. Holz, C. Gorecki, K. Rieck, and F. C. Freiling, "*Measuring and Detecting Fast-Flux Service Networks*", in Proceedings of the Network and Distributed System Security Symposium, San Diego, California, USA, February 2008.

E. Stinson and J. Mitchell, "*Towards systematic evaluation of the evadability of bot/botnet detection methods*", in Proceedings of the USENIX Workshop on Offensive Technologies, San Jose, CA, USA, July 2008.

Meisam Eslahi, Salleh Rosli, and Anuar Nor Badrul. "*Bots and botnets: An overview of characteristics, detection and challenges*", Control System, Computing and Engineering (ICCSCE), 2012 IEEE International Conference on. IEEE, 2012.

M. Feily, A. Shahrestani, and S. Ramadass, "*A Survey of Botnet and Botnet Detection*", in Proceedings of the 3th International Conference on Emerging Security Information, Systems and Technologies, Athens, Greece, June 2009.

Z. Zhu, G. Lu, and Y. Chen, "Botnet Research Survey", in Proceedings of the 32th Annual IEEE International Conference on Computer Software and Applications, Turku, Finland, August 2008.

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 USENIX Security Symposium, pp. 139–154, San Jose, CA, USA, 2008.

J. Oikerinen and D. Reed, "*Internet Relay Chat protocol*", Web publication, http://tools.ietf.org/html/rfc1459#section-1, 2006.

P. Wang, S. Sparks, and C. Zou, "*An Advanced Hybrid Peer-to-Peer Botnet*", IEEE Transactionon Dependable and Secure Computing, vol. 7, no. 2, pp. 113–127, 2010.

J. Liu, Y. Xiao, K. Ghaboosi, H. Deng, and J. Zhang, "*Botnet: Classification, Attacks, Detection, Tracing, and PreventiveMeasures*", EURASIP Journal on Wireless Communications and Networking, vol. 2009, no. 692654, 2009.

S. S. C. Silva, R. M. P. Silva, R. C. G. Pinto, R. M. Salles, "*Botnets: A survey*", Computer Networks: The International Journal of Computer and Telecommunications Networking, vol. 57, no. 2, PP. 378–403, February 2013.

C. Phua, C. Eng-Yeow, Y. Ghim-Eng, S. Kelvin, and N. Minh-Nhut, "*Feature Engineering for Click Fraud Detection*", in Proceedings of the 2012 Workshop on Fraud Detection in Mobile Advertising (FDMA), November 2012.

Butler W. Lampson, "*A note on the confinement problem*" Communications of the ACM, pp. 613-615,.1973.

Lili Qiu, Yin Zhang, Feng Wang, Mi Kyung, and Mahajan Han Ratul, "*Trusted computer system evaluation criteria*", In National Computer Security Center. 1985.

J. Desimone, D. Johnson, B. Yuan, and P. Lutz, "*Covert Channel in the BitTorrent Tracker Protocol*", (2012).

Department of Defence, "Department of defence trusted computer system evaluation criteria", Technical Report, December, 1985.

C. H. Rowland, "Covert channels in the TCP/IP protocol suite", 1997.

M. Antonakakis, R. Perdisci, and et al. "*From throw-away traffic to bots: detecting the rise of DGA-based malware*" , in Proceedings of 21th USENIX Security Symposium, Bellevue, WA, USA, pp. 24–40, August 2012.

D. Dittrich, "*So you want to take over a botnet*", in Proceedings of the 5th USENIX conference on Large-Scale Exploits and Emergent Threats, pp. 6–6. USENIX Association, April 2012.

E. Athanasopoulos, A. Makridakis, and S. Antonatos, "*Antisocial Networks: Turning a Social Network into a Botnet*", in Proceedings of the 11th International Conference on Information Security, pp. 146–160, Taipei, Taiwan, 2008.

Nazario, J.: Twitter based botnet command and control, http://asert.arbornetworks.com/2009/08/twitter-based-botnet-command-channel, 2009.

E. J. Kartaltepe, J. A. Morales, S. Xu, , and R. Sandhu, "*Social Network-Based Botnet Command- and-Control: Emerging Threats and Countermeasures*", in Proceedings of the 8th International Conference on Applied Cryptography and Network Security, pp. 511–528, Beijing, China, 2010.

J. Selvi, "*Covert Channels over Social Networks*", SANS Institute, March 2012.

S. Nagaraja, A. Houmansadr, P. Piyawongwisal, V. Singh, P. Agarwal, and N. Borisov, "*Stegobot: A covert social network botnet*", in Proceedings of the 13th International Conference on Information Hiding, pp. 299–313, Prague, Czech Republic, 2011.

S. Nagaraja, R. Anderson, *"The snooping dragon: social-malware surveillance of the Tibetan movement"* Technical Report, University of Cambridge, March 2009.

K. Solanki, A. Sarkar, and B. S. Manjunath, "*YASS: Yet Another Steganographic Scheme that Resists Blind Steganalysis*", in Proceedings of the 9th International Conference on Information Hiding, pp. 16–31, Saint Malo, France, 2007.

V. T. Lam, S. Antonatos, P. Akritidis, and K. G. Anagnostakis. Puppetnets: mis-using web browsers as a distributed attack infrastructure. In CCS '06: Proceedings of the 13th ACM conference on Computer and communications security, pages 221–234, New York, NY, USA, 2006.

Y. Boshmaf, I. Muslukhov, K. Beznosov, and M. Ripeanu, "*Design and analysis of a social botnet*", published in Computer Networks, pp. 556-578, 2013.

OpenDNS, "The role of DNS in botnet command and control", security white paper, 2012.

Christian J. Dietrich, Christian Rossow, Felix C. Freiling, Herbert Bos, Maarten van Steen, and Norbert Pohlmann, "*On Botnets That Use DNS for Command and Control*", in Proceedings of the Seventh European Conference on Computer Network Defense, PP. 9-16, IEEE Computer Society Washington, DC, USA, 2011.

Antonio Nappa, Aristide Fattori, Marco Balduzzi, Matteo Dell'Amico,and Lorenzo Cavallaro, "*Take a deep breath: a stealthy, resilient and cost-effective botnet using skype*", in Proceedings of the 7th international conference on Detection of intrusions and malware, and vulnerability assessment, PP. 81-100, Springer-Verlag Berlin, Heidelberg, 2010.

Skynet, a Tor-powered botnet: https://community.rapid7.com/community/infosec/blog/2012/12/06/skynet-a-tor-powered-botnet-straight-from-reddit.

Mevade and Sefnit: Stealthy click fraud: http://blogs.technet.com/b/mmpc/archive/2013/09/25/mevade-and-sefnit-stealthy-click-fraud.aspx.

Nicholas Hopper, "Protecting *Tor from botnet abuse in the long term*", Tor Tech Report 2013-11-001, November 20, 2013.

A. Raihana Syahirah, "*Revealing the Criterion on Botnet Detection Technique*". IJCSI International Journal of Computer Science, vol. 10, no. 3, p.p 208-215, 2013.

V. Natarajan, S. Sheen, and R. Anitha, "*Detection of Stegobot : A covert social network botnet*," in Proceedings of the 1st International Conference on Security of Internet of Things, pp. 36–41, Kollam, India, 2012.