فصلنامه علوم و فنون نظامی/ سال نهم/
شماره ۲۳، بهار ۱۳۹۲
صص ۷۲-۵۵

تاریخ دریافت مقاله: ۱۳۹۱/۰۱/۱۵
تاریخ پذیرش مقاله: ۱۳۹۲/۰۳/۲۰

حملات سایبری مبتنی بر شبکه‌های بات و راه‌های مقابله با آن

سلمان کریمی [۱]
عباس مهدوی‌کیا[۲]

چکیده:

یکی از تهدیدات روزافزون در اینترنت و شبکه‌های کامپیوتری، شبکه‌های بات می‌باشد. یک شبکه بات شبکه‌ای از کامپیوترهای آلوده‌ی متصل به اینترنت است که تحت کنترل سرور دستور و کنترل[۳] قرار دارند و برای حملات اینترنتی همچون حملات ممانعت از سرویس[۴] و فرستادن هرزنامه مورد استفاده قرار می‌گیرند. شبکه-های بات با شناسایی سیستم‌های آسیب‌پذیر موجود در شبکه و به مصالحه در آوردن آنها، حیطه‌ی تحت کنترل خود را گسترش می‌دهند. شبکه‌های بات به سرعت در حال پیشرفت هستند و از تکنولوژی‌های جدید همچون تغییرات پی‌درپی سریع یا نظیر به نظیر برای به دام انداختن کاربران و افزایش حفاظت از کامپیوترهای آلوده خود بهره می‌برند. در این مقاله ضمن معرفی مفاهیم مرتبط با شبکه های بات، نحوه-ی ایجادو انتشار آن‌ه در سامانه های نیروهای مسلح جمهوری اسلامی ایران بررسی گردیده و درنهایت پیشنهادهایی برای افزایش امنیت شبکه های مورد استفاده در نیروهای مسلح ارائه گردیده است.

کلید واژه‌ها: امنیت شبکه،جنگ سایبری، شبکه‌های بات[۵]

---

۱ - عضو هیئت علمی دانشکده رایانه و فناوری اطلاعات دانشگاه هوایی شهیدستاری karimiemail@yahoo.com

۲ – کارشناس ارشد مدیریت بازرگانی مدرس دانشگاه هوایی شهید ستاری

۳ -Command &Control
۴ -Denail of Service
۵ -Bot Nets

۱ - مقدمه

واژه امنیت[۱]عبارت است از به حداقل رساندن آسیب‌پذیری منابع و سرمایه‌ها. امنیت مبتنی بر تحقق سه ویژگی محرمانگی[۲]، جامعیت[۳] و دسترس‌پذیری[۴] در یک سیستم است. یکی از تهدیدات روزافزون در اینترنت و شبکه‌های کامپیوتری که اصل دسترس‌پذیری را نقض می‌کند، شبکه‌های بات می‌باشد. شبکه بات شبکه‌ای از کامپیوترهای آلوده است که متصل به اینترنت می‌باشند و برای حملات توزیع شده اینترنتی مانند ممانعت از سرویس[۵]، مورد استفاده قرار می‌گیرند. گستردگی ارتباطات، به اشتراک گذاری منابع، حس کنجکاوی، کسب پول، جمع‌آوری اطلاعات و بدست آوردن ظرفیت منابع، انگیزه‌هایی برای ایجاد شبکه‌های بات است. به عنوان مثال در سال ۲۰۰۹ سایت‌های مخصوص شبکه‌های اجتماعی همچون Twitter،Facebook، Livejournal و صفحات بلاگ گوگل مورد تهاجم حملات ممانعت از سرویس توزیع شده[۶] قرار گرفتند. یا حمله مشابه‌ای که در سال ۲۰۱۰ برروی سازمان‌های بزرگی همچون Visa.com،PayPal.com،Mastercard.com و PostFinance صورت گرفت و باعث شد تا وب‌سایت‌های مخصوص این سازمان‌ها از ارائه سرویس باز بمانند.

تعداد شبکه‌های بات روزانه در حال افزایش است و از طرفی سازندگان چنین شبکه‌هایی به فناوری‌ها و تکنیک‌های جدید همچون DNS (C.Brandhorst۲۰۰۶:۳-۱)و تغییرات پی‌درپی سریع(E. Passerini,۲۰۰۸ : ۵)،(J. Nazario, ۲۰۰۸:۱-۵) روی آورده‌اند. بر اساس گزارشاتی که مرکز امنیتی کسپرسکی[۷] در وب سایت این مرکز قرار داده است،(http://www.securelist.com/en/analysis/۲۰۴۷۹۲۱۸۰/TDL۴_Top_Bot دسترسی در ۱۰ /۱۳۹۲/۲) . تعداد قربانیان (بات‌ها) شبکه بات TDL۴ در حدود ۴,۵ میلیون عدد تخمین زده شده است. این مسئله قدرت شبکه‌های بات را بیش از پیش نشان می‌دهد. چراکه مهاجم می‌تواند با در اختیار داشتن چنین لشکر انبوهی، به هر مقصدی به سادگی حمله کند.

امروزه در مراکز امنیتی و نظامی نیز دسترسی به سرویسهای اینترنت و یا اینترانت ملی

۱-Security
۲-Confidentiality
۳-Integrity
۴-Availability
۵-Denial of Service
۶-Distributed Denail of Service
۷-Kaspersky

اجتناب ناپذیر است و لذا مقابله با بات ها لازم است در اولویت قرار گیرد چرا که خسارات ناشی از بات‌ها برای این مراکز به مراتب بیشتر از هکرها و نفوذگران خواهد بود. بعد از هر نفوذ توسط نفوذگران بلافاصله می‌توان حفره‌های امنیتی را پوشش داد ولی در صورت آلودگی به بات‌ها می‌توان ادعا کرد که در یک زمان بسیار کوتاه خسارات امنیتی جبران ناپذیری وارد خواهد شد.

۱ - تعریف شبکه‌های بات

بات کلمه‌ای برگرفته از روبات اینترنتی[۱] می‌باشد و به برنامه‌هایی گفته می‌شود که برای اجرای وظایف خودکار بر روی اینترنت طراحی شده‌اند و انجام کارهای تکراری و ساده بر عهده آن‌ها می‌باشد.(Samuel Greengard,۲۰۱۲:۲)

بات دو مورد استفاده دارد:

-**کارکرد خوب:** به عنوان عامل‌های هوشمند در موتورهای جستجو و بازی‌های آنلاین

-**کارکرد بد:** دزدی اطلاعات، حملات ممانعت از سرویس، هرزنامه و دیگر حملات

در این مقاله بات‌ها به مفهوم برنامه‌های نرم‌افزاری هستند که بر روی کامپیوتر قربانی اجرا می‌شوند و کنترل کامل فعالیت‌های میزبان را به صورت از راه دور در اختیار فرد سودجو قرار می‌دهند، بدون اینکه میزبان از این موضوع اطلاعی داشته باشد. کامپیوتر قربانی یک میزبان اینترنتی آسیب‌پذیر است که بعد از این‌که حمله کننده با شناسایی آسیب‌پذیری موجود در سیستم کاربر و یا با ترغیب کردن او به اجرای یک برنامه مخرب[۲]، بات را بر روی سیستم نصب می‌کند و آن را به یک سیستم آلوده تبدیل می‌نماید (Manoj. Rameshchandra Thakur۱,۲۰۱۲:۴-۵). حمله کننده به دنبال قربانیانی است که به اینترنت وصل هستند، فعالیت آن‌ها کمتر بازرسی می‌شود، پهنای باند بالایی دارند و عموما کامپیوترهای شخصی خانگی و یا سرورهای دانشگاهی هستند. چند ویژگی در انتخاب قربانی مهم است: پهنای باند زیاد، دسترس‌پذیری، آگاهی پایین کاربر (به روز نبودن سیستم‌عامل و برنامه‌های کاربردی، نبودن تجهیزات کنترل دسترسی مانند دیواره‌آتش[۳] از پیامدهای آگاهی کم کاربران است).

۱-Internet Robot

۲-Malicious

۳-Firewall

این ویژگی‌ها این امکان را برای حمله کننده فراهم می‌آورد تا به راحتی وارد سیستم شود و به مدت طولانی‌تری بات‌ها را از خطر کشف و ردیابی محافظت نماید. بات دستورات خود را از سرور دستور و کنترل[۱] که توسط حمله کننده[۲]هدایت می‌شود، دریافت می‌نماید.حمله کننده معمولا فردی است که تمامی کارهای یک شبکه بات، از ایجاد تا کنترل را در دست داشته و بات را پیکربندی می‌کند و روش‌هایی که برای مصالحه کردن سیستم قربانی به کار می‌رود را مشخص کرده و آن‌ها را پیاده‌سازی می‌نماید. سپس بات را بر روی سیستم قربانی نصب و در نهایت آنها را از طریق کانال کنترلی[۳] هدایت و رهبری می‌کند و دستورات حمله را صادر می‌نماید. حملات متنوعی توسط شبکه‌های بات صورت می‌گیرد، در ادامه به برخی از حملات مهم پرداخته‌ایم.

۱. **حملات توزیعی ممانعت از سرویس:** حمله کننده با دستور دادن به تمامی بات‌ها می‌تواند ترافیک گسترده‌ی را روانه سیستم قربانی نماید که در نتیجه قربانی از انجام وظیفه خود و ارائه خدمات باز می‌ماند.

۲. **آلودگی مرتبه دوم**[۴]: با نصب بات، حمله کننده کنترل کامل ماشین قربانی را در دست می‌گیرد، بدین ترتیب حمله کننده می‌تواند key logger یا تروجان[۵] را دانلود و نصب نماید و اطلاعات ارزشمند قربانی را از طریق این سیستم آلوده به سرقت ببرد. این اطلاعات می‌تواند شامل کلمات عبور کارت‌های بانکی، کارت‌های اعتباری یا اطلاعات شخصی ذخیره شده در سیستم باشد.

۳. **درپشتی**[۶]: بات‌ها بر روی ماشین‌های قربانی به عنوان درپشتی نصب می‌شوند و امکان دسترسی به سیستم قربانی را بعد از سوءاستفاده از آسیب‌پذیری فراهم می‌سازند، به طوریکه حمله کننده می‌تواند بات‌ها را به گونه‌ای پیکربندی نماید که از همان پورت‌های ترافیک قانونی استفاده نماید و شانس کشف را کاهش دهد.

۴. **میزبانی داده و اطلاعات غیرقانونی:** حمله کننده‌ها در استفاده‌ای گسترده، از بات‌ها برای مشارکت سیستم قربانی در شبکه‌های به اشتراک گذاری فایل و دیگر فضاهای

۱-Command and Control
۲-Botmaster
۳-Control channel
٤-Secondary local infection
٥-Trojan
٦-Backdoor

ذخیره‌سازی برای میزبانی فایل‌های غیرقانونی، نرم افزار یا فیلم‌های دزدی استفاده می‌نمایند.

۲ - نحوه ایجاد شبکه بات

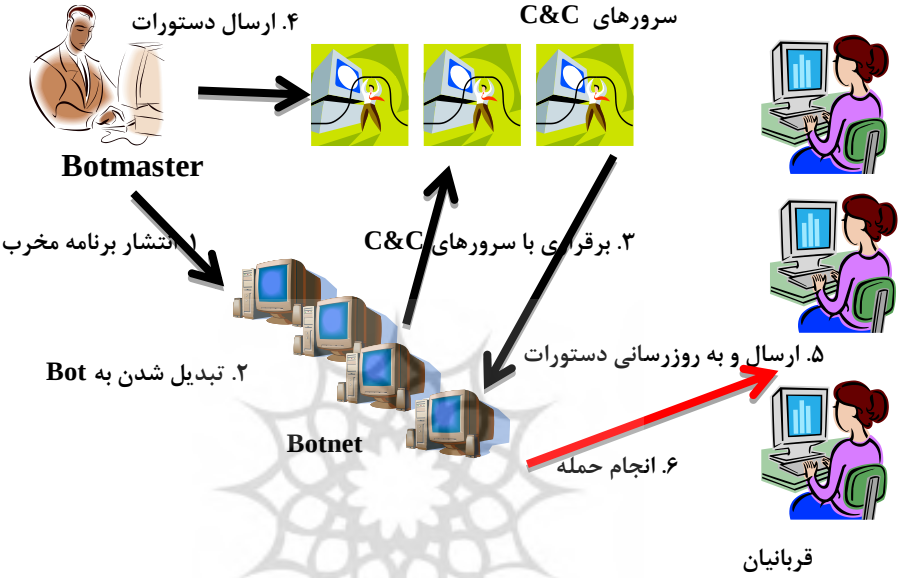
نحوه انجام این مرحله بستگی به مهارت‌ها و نیازمندی‌های حمله کننده دارد. ممکن است حمله کننده کدی را که خودش نوشته، انتخاب کند و یا کد مربوط به بات دیگری را که قبلا نوشته شده است، گسترش بدهد و از آن استفاده کند. البته یک‌سری از بات‌ها نیز به صورت آماده قابل خریداری هستند. کد بات، دارای اجزایی است که قابلیت پیکربندی و اعمال تنظیمات دلخواه حمله کننده را دارد. این اجزا عبارتند از: اطلاعات سرور کنترل و دستور، اطلاعات کانال ارتباطی، پورت سرویس TCP از راه دور، مکان و نام فایل کد بات که بر روی ماشین آلوده قرار دارد و اجزایی که به حمله کننده این امکان را می‌دهد تا به صورت پویا حمله را تغییر دهد و لیست حمله کنندگان و اطلاعات مربوط به آن‌ها را پنهان سازد(G. Ollmann,۲۰۰۹:۵-۴)

نحوه انتشار بات

این مرحله بر روی سیستم‌های آسیب‌پذیر و ابزارهایی که برای سوءاستفاده از آسیب-پذیری‌های آن‌ها استفاده می‌شود، تمرکز دارد. این ابزارها امکان دسترسی درپشتی را فراهم می‌آورندو به نصب بات سرعت می‌بخشند. مرحله انتشار بات و آلوده ساختن ماشین‌های قربانی شامل تکنیک‌های مختلفی است. یکی از این روش‌ها استفاده از تکنیک‌های مهندسی اجتماعی[۱] است، همچون فرستادن پست‌های الکترونیکی، پیغام‌های کوتاه و محتوای وب مخرب. برنامه بات از طریق شبکه‌های به اشتراک گذاری فایل نیز انتشار می‌یابند مانند دریافت و باز کردن فایل آلوده به اشتراک گذاشته شده. برنامهبات از پروتکل‌هایی همچون FTP ، HTTP و TFTP بهره می‌برد تا کامپیوترها را آلوده ساخته و انتشار یابد. این کار تا زمانی ادامه می‌یابد که شبکه بات به اندازه کافی و متناسب با هدف حمله کننده گسترش یابد. در شکل۱ نحوه ایجاد شبکه بات مشاهده می‌شود:

۱-Social engineering

مرحله (۱): حمله کننده سعی دارد تا ماشین‌های قربانی را با استفاده از بات‌ها و از طریق افشای آسیب‌پذیری‌های موجود در برنامه‌های کاربردی[۱] و یا سیستم عامل، آلوده سازد و یا کاربر را فریب دهد و او را ترغیب به اجرای یک برنامه کاربردی مخرب بنماید که منجر به نصب بات می‌شود.



شکل (۱) - نحوه ایجاد شبکه بات

مرحله (۲): یکی از راه‌ها و روش‌های اصلی آلوده کردن گروه زیادی از میزبان‌های اینترنتی، استفاده از کد افشای آخرین آسیب‌پذیری است که هنوز برطرف نشده است. با استفاده از این آسیب‌پذیری می‌توان به ماشین قربانی دست یافت و بات را به عنوان درپشتی[۲] نصب کرد. فرایندی که توضیح داده شده و می‌تواند به صورت خودکار و یا توسط یک کرم[۳]هدایت شده انجام گیرد. با کمک این کرم یک زیرشبکه مورد بررسی قرار می‌گیرد تا آسیب‌پذیری-های آن یافت شود و سیستم‌های آسیب‌پذیر بوسیله بات آلوده شوند. بعد از اینکه بات بر روی ماشین قربانی نصب شد، خودش را در دایرکتوری نصب، کپی می‌نماید.

مرحله (۳): بات سعی می‌کند تا به سرور دستور و کنترل وصل شود. سرور دستور و کنترل، نیز سیستمی است که حمله کننده برای کنترل و فرستادن دستورات خود به بات‌ها استفاده

۱-Application
۲-Backdoor
۳-Worm

می‌کند. حمله کننده دستورات جدید را بر روی این سرور قرار می‌دهد، بدین ترتیب بات‌ها دستورات را دریافت و حملات را انجام می‌دهند.

مرحله(۴): زمانی‌که بات بر روی ماشین قربانی نصب می‌شود، با استفاده از کلمه کلیدی یکتا، خود به عنوان بخشی از شبکه حمله کننده، به کانال وصل می‌شود و منتظر رسیدن دستورات می‌ماند. کانال کنترلی که توسط حمله کننده ایجاد می‌گردد، به عنوان نقطه‌ی وعدگاه و قرارگاه تمامی بات‌ها به شمار می‌آید به طوری‌که هر بات بعد از نصب شدن خود بر روی سیستم قربانی، به صورت خودکار سعی می‌کند تا به این کانال وصل شود.

مرحله(۵): پس از آن‌که این بات‌ها به کانال کنترلی حمله کننده وصل می‌شوند، حمله کننده بوسیله‌ی یک کلمه عبور مخصوص وارد این بات‌ها می‌شود. بدین ترتیب اطمینان می‌یابد که بات‌ها نمی‌توانند توسط افراد دیگری کنترل شوند و از خطر دزدیده شدن در امان هستند. بعد از این‌که دسترسی مورد قبول واقع شد، حمله کننده فعالیت تعداد زیادی از سیستم‌های آلوده را از طریق شبکه بات به صورت مستقیم یا از راه دور بدست می‌گیرد.

مرحله(۶): در نهایت همه چیز برای انجام حملات مورد نظر آماده است.

تکنیک‌های کنترل و دستورشبکه‌های بات

تکنیک‌های کنترل و دستور مختلفی در شبکه‌های بات مورد استفاده قرار می‌گیرد(.K Yuji,۲۰۰۷:۵-۶) که در این بخش آن‌ها را توضیح می‌دهیم. همان‌طور که اشاره شد زمانی که بات بر روی ماشین‌های قربانیان نصب می‌گردد، حمله کننده باید این ماشین‌های آلوده را بیابد و کنترل آن‌ها را به عهده بگیرد. یکی از ساده‌ترین روش‌های ممکن ارتباط مستقیم بین حمله کننده و بات‌ها می‌باشد. با وجود این لینک مستقیم، می‌توان به آسانی حمله کننده را ردیابی کرد. حمله کننده به دلیل امنیت پایین این روش، از آن استفاده نمی‌کند و به جای آن تکنیک‌های کنترل و دستور زیر را برای کنترل از راه دور به کار می‌برد.

۱ - تکنیک متمرکز[۱]

این تکنیک از یک سرور مرکزی با پهنای باند زیاد برای میزبانی استفاده می‌نماید تا پیغام‌ها را مابین بات‌های مختلف انتقال دهد. سرور دستور و کنترل در شبکه‌های بات، یک ماشین آلوده است که از پروتکل‌هایی همچون IRC یا HTTP برای ارائه سرویس استفاده

۱-Centeralized

می‌نماید. نوع متمرکز سرور دستور و کنترل از متداول‌ترین تکنیک‌ها می‌باشد که بسیاری از بات‌ها از آن بهره می‌گیرند. از مهم‌ترین مزایای استفاده از تکنیک دستور و کنترل متمرکز، قابلیت دسترسی‌پذیری بالا، برقراری ارتباط آسان با آن، کم بودن تاخیر پیغام‌ها و توان کنترل تعداد بیشماری از بات‌ها می‌باشد. منابع متعددی برای برپایی چنین سرورهایی موجود است. یکی از متدوالترین نوع‌ها سرورهای IRC هستند. تنها نقطه ضعف این تکنیک همین سرور مرکزی کنترل و دستور است، به این دلیل که تمامی ارتباطات از این نقطه گذر می‌کنند و با کشف این سرور مرکزی ارتباط بین اعضای شبکه بات قطع شده و کل شبکه از کار می‌افتد.

۲ - تکنیک نقطه به نقطه[۱]

برخلاف سیستم‌های متمرکز که یک سرور مرکزی به عنوان سرویس‌دهنده خدمات عمل می‌کند، در این معماری سرور مرکزی وجود ندارند. تمامی کامپیوترهای عضو چنین شبکه‌ای هم به عنوان سرویس گیرنده[۲] عمل می‌کنند و هم به عنوان سرویس دهنده[۳]. هر کامپیوتر سرویس گیرنده می‌تواند به طور مستقیم با هر کدام از کامپیوترهای سرویس گیرنده دیگر ارتباط برقرار کند. این مدل به نام مدل شبکه نقطه به نقطه شناخته می‌شود. هدف اصلی این مدل، قادر ساختن تمامی کامپیوترهای سرویس گیرنده به انتقال فایل به دیگر کامپیوترها می‌باشد. برای همین است که چنین شبکه‌هایی اغلب «شبکه‌های به اشتراک‌گذاری فایل» نیز نامیده می‌شوند زیرا تمامی کاربران شبکه را قادر می‌سازد تا هم فایل مورد نظر را از دیگر کاربران درخواست کند و هم فایل خود را برای آن‌ها ارسال نماید. به این دلیل که در این مدل هیچ نیازی به وجود سرور مرکزی برای انتقال پیغام‌ها نیست و کشف آن دشوار است. با استفاده از این تکنیک پایداری شبکه نیز افزایش می‌یابد چرا که با از کار افتادن یکی از کامپیوترها، کامپیوترهای دیگر کار آن را به عهده می‌گیرند و شبکه قادر به ادامه ارائه سرویس خود خواهد بود. قابل ذکر است که اندازه شبکه‌های باتی که با سیستم نقطه به نقطه پشتیبانی می‌شوند، کوچک می‌باشند. از ضعف‌های این روش می‌توان به تاخیر انتشار و نبود تضمین در رسیدن پیغام اشاره کرد.

۱-Peer to Peer

۲-Client

۳-Server

۳ -تکنیک تصادفی[۱]

در این تکنیک حمله کننده به یکی ازبات‌ها پیغام رمزشده را به طور تصادفی می‌فرستد. هر بات تنها از وجود یک بات دیگر اطلاع دارد که این ارتباط می‌تواند توسط بات دیگری قطع شود و یک ارتباط دیگری شروع گردد. بدین ترتیب کشف این نوع شبکه‌های بات بسیار دشوار است. در این نوع مکانیزم تاخیر انتشار بسیار بالا می‌باشد و تضمینی برای رسیدن پیغام نیست. تاکنون هیچ شبکه باتی یافت نشده است که از این تکنیک بهره ببرد.

۴ - پروتکل‌های مورد استفاده در شبکه‌های بات

همان‌گونه که اشاره شد، حمله کننده برای ارسال دستورات خود از سرورهای دستور و کنترل استفاده می‌نماید. امروزه پروتکل‌های مختلفی برای برقراری ارتباط بین سرور دستور و کنترل و اعضای شبکه‌های بات استفاده می‌شود(R. Villamarin-Salomon, ۲۰۰۸:۲-۳)، (D. Dagon, ۲۰۰۵:۷).

۱- پروتکل IRC

یکی از پرکاربردترین پروتکل‌ها IRC[۲] می‌باشد. پروتکل IRC به کاربران امکان برقراری ارتباط با یکدیگر را می‌دهد. این پروتکل به صورت متمرکز کار می‌کند، بدین معنا که یک سرور مرکزی به کاربران سرویس می‌دهد و اطلاعات مورد نیاز کاربران را در اختیارشان قرار می‌دهد. سرور مرکزی برای ارتباط کاربران اتاق‌های گفتمان فراهم می‌آورد که به آن‌ها کانال نیز گفته می‌شود. هر کاربری که قصد دارد تا به یکی از کانال‌ها متصل گردد، از یک نام کاربری یکتا استفاده می‌نماید که به آن nickname می‌گویند. شبکه بات مبتنی بر پروتکل IRC به صورت push عمل می‌نماید. در رویکرد push، دستورات روانه کانال‌های ارتباطی می‌شوند و هر بات متصل به کانال‌ها دستورات را دریافت می‌نماید.

۲- پروتکل HTTP

از متدهای دیگری که برای کنترل و فرستادن دستور توسط حمله کننده به کار می‌رود، پروتکل HTTP است. به این دلیل که استفاده از پروتکل IRC توسط شبکه‌های بات متداول

۱-Random

۲-Internet relay chat

است، بیشتر تکنیک‌های کشف این شبکه‌ها بر روی تحلیل ترافیک IRC متمرکز هستند و ترافیک HTTP را نادیده می‌گیرند. این پروتکل نیز به صورت متمرکز عمل می‌نماید، بدین معنا که یک سرور مرکزی ثابت وجود دارد که سیستم‌های آلوده با آن ارتباط برقرار می‌کنند و دستورات حمله را از این سرور دریافت می‌نمایند.

در شبکه‌های بات مبتنی بر HTTP رویکرد pull به کار برده می‌شود. سیستم آلوده سعی می‌کند تا با سرور مبتنی بر وب ارتباط برقرار کند و آدرس IP خود را به اطلاع سرور برساند و اعلام دارد که بر روی چه پورتی پروکسی اجرا می‌شود و همچنین رشته شناسه ماشین که برای شناسایی و ارتباط با بات استفاده می‌شود را ارائه دهد. چون ارتباط مابین بات‌ها و سرور دستور و کنترل پایدار نیست، بنابراین بات به صورت دوره‌ای در فواصل زمانی منظم تماس برقرار می‌کند و دستورات را در قالب پاسخ‌های HTTP دریافت می‌نماید.

۳- شبکه‌های ضد اجتماعی[۱]

سیستم‌های توزیع شده‌ای مبتنی بر شبکه‌های اجتماعی هستند که حمله کننده می‌تواند از آن‌ها سوءاستفاده کند و حملات شبکه‌ای انجام دهد. سه خصوصیت مهم شبکه‌های اجتماعی که توجه حمله کننده‌ها را به خود جلب کرده است از این قرار است:

- پایگاهی توزیع شده و بزرگ از کاربران
- دسته‌هایی از کاربران که علاقمندی‌های یکسان خود را به اشتراک گذارده‌اند و اعتمادی بین خود به وجود آورده‌اند و به منابع یکسانی دسترسی دارند
- وجود سکویی آزاد برای تولید منابع و برنامه‌های کاربردی فریب دهنده

در گزارشات اخیر مشاهده شده است که شبکه‌های اجتماعی همچون Twitter و Facebook مورد توجه حمله کنندگان قرار گرفته‌اند. در این نوع حملات، بات خود را عضو شبکه اجتماعی می‌نماید. دستورات به صورت پست‌های متداول در این شبکه‌های اجتماعی به بات ابلاغ می‌شود.

۴- پروتکل نقطه به نقطه

این پروتکل در شبکه‌های نقطه به نقطه مورد استفاده قرار می‌گیرد. در این شبکه‌ها برای انتقال پیغام‌ها هیچ نیازی به وجود سرور مرکزی نیست. حمله کنندگان با استفاده از این

---

۱ -Antisocial

پروتکل از مزایای زیر برخودار می‌شوند: هر گروهی که عضو شبکه می‌باشد منبعی برای پهنای باند، حافظه و قدرت پردازشی است. داشتن چنین منابعی، این قدرت را به حمله کننده می‌دهد تا حملات ممانعت از سرویس توزیع شده را به طور گسترده‌تری انجام دهد. همچنین حجم زیادی از هرزنامه‌ها را به سمت قربانیان بفرستد.

۵-مکانیزم DNS

حمله‌کننده در مرحله نگهداری، برای به روزرسانی بات‌ها و جلوگیری از از کار افتادن سرور از مکانیزم DNS استفاده می‌کند(R.Villamarin-Salomon,۲۰۰۸:۲). در واقع بات برای برقراری ارتباط با سرور مرکزی از سرور DNS پرس و جو می‌کند و آدرس IP متناظر با URL سرور را بدست می‌آورد. DNS، کمک می‌نماید تا در صورت از کار افتادن سرور مرکزی، بتوان سرور دیگری را جایگزین آن کرد و آدرس IP سرور جایگزین را در اختیار بات قرار داد.

۵ - روش‌های مقابله با شبکه‌های بات

شبکه‌های بات با استفاده از ابزارهای جدید و بهبود یافته و انجام حملات متعدد، چالشی جدی در اینترنت بوجود آورده است. جلوگیری از به دام افتادن قربانی در شبکه‌های بات و کشف مکان حمله کننده، کاری بسیار چالش برانگیز است زیرا اولا مکانیزمی که در ساخت و نگهداری شبکه‌های بات استفاده می‌شود و همچنین روشی که برای حمله به کار برده می‌شود، مستقل از هم می‌باشند. ثانیا هر کامپیوتر آلوده که در یک شبکه بات می‌باشد، منبعی برای حمله است و ثالثا شبکه‌های بات تا آغاز یک حمله خاص، در حالت سکوت باقی می‌مانند.

جلوگیری از آلودگی سیستم به بات نیازمند سطح بالایی از آگاهی در مورد امنیت و حریم خصوصی[۱] می‌باشد. علاوه بر این، سیستم همواره باید به روز باشد و تمامی به روزرسانی‌ها و فایل‌های patch سیستم عامل نصب شده باشند. به کار بردن بازی‌ها و نرم-افزارها بدون کسب اجازه ناشر[۲] و دیگر تجهیزات غیرقانونی آنلاین، همواره منبع کدهای مخرب هستند و تهدید امنیتی جدی به شمار می‌آیند و کاربران باید از بازدید چنین

۱-Privacy
۲-Pirated

سایت‌هایی خودداری کنند. دیواره‌های‌آتش و برنامه‌های ضد ویروس/ ضد جاسوس‌افزار[۱] باید بر روی سیستم‌های نصب گردند و به صورت دوره‌ای به روزرسانی شوند تا از آلوده شدن سیستم خودداری نمایند.(M. Bailey,۲۰۰۹: ۳)

کشف فعالیت بات بر روی سیستم یا شبکه، حوزه بسیار گسترده‌ای برای مطالعه می‌باشد. تکنیک‌های منفعل[۲] و فعال[۳] متعددی پیشنهاد شده‌اند تا این شبکه‌ها را شناسایی کرده و کشف نمایند. یکی از راه‌های کشف آن‌ها بررسی و تحلیل ترافیک شبکه و فعالیت میزبان می‌باشد؛ مانند بررسی تعداد کاربران به ازای پورت‌های سرویس کانال و یا بررسی نسبت تعداد کاربران غیرقابل تشخیص[۴] به تعداد کاربران نمایان و قابل رویت[۵]. هدف برخی از رویکردها کشف سرورهای دستور و کنترل و از کار انداختن آن‌ها می‌باشد که عموما از طریق تحلیل مشخصات جریان‌ها مانند بررسی پهنای باند، طول مدت ارتباط و زمانبندی، کار خود را انجام می‌دهند. روش‌های دیگری بر پایه سه معیار ارتباط، پاسخ و همزمانی پیشنهاد شده‌اند که از طریق تحلیل‌های رفتاری، شبکه‌های بات را کشف می‌نمایند.

سیستم‌های کشف مبتنی بر امضا

از روش‌های مبتنی بر امضا می‌توان برای کشف کانال‌های ارتباطی مابین بات و حمله-کننده استفاده کرد.(J. Goebel,۲۰۰۷:۲) در این سیستم‌ها تمرکز بر روی پروتکل IRC است.(ibid.) در شبکه‌های بات مبتنی بر IRC، با کشف سرور مرکزی می‌توان شبکه بات را از کار انداخت. اما مشکلی که به وجود می‌آید این است که با خاموش شدن سرور و قطع ارتباط مابین بات‌ها و حمله کننده دیگر به بات‌ها دسترسی نداریم و آن‌ها بدون این‌که پاک شوند آلوده خواهند ماند. بنابراین در این مطالعه هدف، کشف کانال‌های ارتباطی IRC است تا با این کار بتوان هم سرور کنترل و دستور و هم بات‌ها را شناسایی کرد. این سیستم از مشخصات پروتکل IRC برای یافتن کانال‌ها استفاده می‌کند. همچنین از معیارهای تشابه برای یافتن شباهت ما بین مشخصات موجود و مشخصات مبتنی بر شبکه‌های بات شناخته شده، بهره می‌برد.

سیستم پیشنهادی این روش، به تمامی بسته‌های گذرنده از شبکه گوش می‌دهد و

۱-Spyware
۲-Reactive
۳-Proactive
٤-Invisible
٥-Visible

هنگامی که بسته‌های شامل دستورات مخصوص پروتکل IRC را می‌بیند، آن بسته‌ها را ثبت کرده و مشخصات آن بسته‌ها را ذخیره می‌کند و سپس آن‌ها را مورد تحلیل قرار می‌دهد. این دستورات IRC شامل عباراتی از قبیل JOIN، NICK، USER،MODE و QUIT است. مشخصاتی که از این بسته‌ها ذخیره می‌گردد شامل زمان ارتباط، آدرس IP و پورت میزبان، آدرس IP و پورت سرور، کانال‌هایی که به آن‌ها پیوسته و utilized nickname می‌باشند.

سیستم‌های مبتنی بر رفتارهای غیرعادی

یکی از رویکردهای اساسی بررسی رفتار و تحلیل ترافیک و پورت‌های مورد نظر بات‌هایی است که برای برقراری ارتباط از پروتکل IRC استفاده می‌کنند. زمانی که سرور تقاضای ارتباط بات را رد می‌کند تمامی بات‌ها در بازه‌های زمانی مشخصی سعی در برقراری ارتباط مجدد می‌کنند. همچنین الگوهای ارتباطی بات‌ها متفاوت از کاربران عادی است. روشهایی نیز برای بررسی و شناساییشبکه‌های بات با محوریت ISP ها وجود دارد.(۳: ۲۰۰۹ ,A Caglayan)این روشها، یک تحلیل منفعل است که مبتنی بر جریان داده می‌باشد. در این رویکردها، بعد از آن‌که میزبان‌های دارای رفتار مشکوک شناسایی شدند، ترافیک ورودی و خروجی آن‌ها متمایز می‌شود. به منظور شناسایی حمله کننده، بر روی این ترافیک تحلیل بیشتری صورت می‌گیرد و پورت‌های ارتباطی مشخص می‌گردند و تحلیل‌های انجام شده به صورت گزارش نمایش داده می‌شوند.

رویکرد دیگر مبتنی بر الگوهای رفتاری مشابه در میانبات‌ها می‌باشد (Ibid) بات در هنگام دریافت دستورات، مشخصه‌های رفتاری خاصی دارد و در پاسخ به دستورات، یک‌سری فعالیت انجام می‌دهد. در این مقاله مطالعه بر روی یک بات در محیط کنترل شده انجام می‌گیرد. در این محیط کنترل شده، سعی می‌شود تا دستوراتی که به این بات می‌رسند و همچنین پاسخ‌هایی که بات در ازای دریافت این دستورات ارائه می‌نماید، شناسایی گردند. سپس این مشاهدات مورد تحلیل قرار می‌گیرند و مدل‌های کشف بات بر مبنای این مشاهدات، ساخته شده و به کار گرفته می‌شوند.

نکته قابل توجه دیگر این است که شبکه‌های بات مشخصات رفتاری و ارتباطی تقریبا ثابت و قابل شناسایی دارند که مستقل از پروتکل دستور و کنترل و ساختار شبکه بات است. (G. Gu ,۲۰۰۸:۵) در حالت کلی بات‌های موجود در یک شبکه بات:

- با سرور ارتباط برقرار می کنند.

- فعالیت‌های مخرب انجام می دهند.
- به صورت مشابه و منسجمی عمل می‌نمایند.

در این رویکرد ترافیک ارتباطی مشابه و ترافیک مخرب مشابه خوشه‌بندی می‌گردد. بر روی دسته‌های بدست آمده نیز خوشه‌بندی انجام می‌دهد تا میزبان‌هایی که الگوهای ارتباطی مشابه و الگوهایرفتاری مخرب مشابه دارند، یافته شوند.

سیستم ارائه شده دو مقوله را بررسی می‌کند:

- چه کسی با چه کسی صحبت می‌کند. بررسی این رفتار باعث آشکار شدن فعالیت‌های ارتباطاتی سرور دستور و کنترل می شود.
- چه کسی چه کاری می‌کند. با تحلیل آن می‌توان فعالیت‌های مخرب را کشف کرد.

به این ترتیب با اجرای خوشه‌بندی در عرض، میزبان‌هایی با الگوهای مشابه یافته می‌شوند.

سیستم‌های مبتنی بر DNS

امروزه حمله کننده‌ها از روش جدید مبتنی بر DNS برای برقراری ارتباط ما بین بات و سرور دستور و کنترل استفاده می‌کنند(C. Hyunsang۲۰۰۷:۳-۴)، (M. Bailey,۲۰۰۹:۴). استفاده از DNS باعث می‌شود تا بات‌ها غیرقابل مشاهده شوند و همچنین قابلیت حمل داشته باشند. از DDNS[۱] نیز می‌توان برای سرویس‌دهی بهتر استفاده کرد تا در صورت خراب شدن سرور، جایگزین دیگری از میان بات‌ها برای آن یافته شود. اما استفاده از سیستم DNS به عنوان IDS[۲] راه‌حل جالبی به نظر می‌رسد، چرا که جمع‌آوری داده‌ی مورد نیاز از این طریق راحت است. تنها مشکلی که وجود دارد تحلیل این داده می‌باشد که کار دشواری است.

دو رویکرد دیگر برای شناسایی سرورهای کنترل و دستور شبکه‌های مبتنی بر DNS نیز وجود دارد.(R. Villamarin-Salomon,۲۰۰۸:۳-۴) رویکرد اول به جستجوی نام دامنه‌هایی می‌پردازد که نرخ پرس‌وجوی غیرعادی بالایی دارند و یا این‌که نرخ به صورت زمانی[۳] متمرکز می‌باشد. دلیل بررسی نرخ پرس‌وجوها این است که حمله کننده غالبا سرور دستور

۱-Dynamic DNS

۲-Intrusion detection system

۳-temporally

و کنترل را تغییر می‌دهد، بنابراین بات‌ها برای تماس با سرور نیازبهمکان‌یابی آن از طریق DNS دارند، بدین ترتیب نرخ بالایی از پرس‌وجوهای DNS نام دامنه مشاهده می‌شود.

رویکرد دوم به دنبال پاسخ‌های DNS غیرعادی مانند NXDOMAIN است(پیغام خطای وجود نداشتن نام مورد نظر که از سمت سرور DNS در پاسخ به پرس و جوی انجام شده، فرستاده می‌شود.). یکی از دلایل تمایل به این رویکرد این است که بات‌ها سعی در یافتن آدرس IP جدید سرور کنترل و دستوری دارند که از کار افتاده است.

راه دفاعی دیگر که مبتنی بر رفتار غیرعادی می‌باشد با بررسی و تحلیل کردن ترافیک DNS، میزبان‌های مشکوک به بات را کشف می‌کند. ایده‌ی اصلی این کار یافتن مشخصه‌ی کار گروهی بات‌ها در ترافیک پرس‌وجوهای DNS است که از سمت این بات‌ها فرستاده می‌شوند.

در این روش یک ویژگی به نام فعالیت گروهی وجود دارد که از آن برای کشف شبکه-های بات استفاده می‌شود. این فعالیت گروهی به ویژگی‌هایی از ترافیک DNS گفته می‌شود، که این ترافیک را متمایز می‌سازد. ویژگی‌های ترافیک DNS شبکه‌های بات این است که سایز ثابت/گروه ثابت (اعضای شبکه بات) همزمان به نام دامنه دسترسی یافته، همزمان مهاجرت کرده و همزمان عمل می‌کنند. به همین دلیل پرس‌وجوهای DNS به صورت زمانی و مشابه رخ می‌دهند. در صورتی که بیشتر ترافیک عادی DNS به صورت متناوب رخ می‌دهد اما هیچ الگوی مشابه ترافیکی نیز مشاهده نمی‌شود.

در سیستم کشف، پایگاه داده‌ای وجود دارد که پرس‌وجوهای DNS را که شامل آدرس IP، نام دامنه و مهر زمانی است، جمع‌آوری کرده و بر اساس نام دامنه و مهر زمانی، آن‌ها را گروه‌بندی می‌کند و سپس سیستم تشابه بین لیست‌های IP نام دامنه‌های مختلف را با الگوریتمی محاسبه می‌کند و در صورت یافتن تشابه، میزبان‌های مشکوک به Bot و همچنین نام دامنه‌های آلوده را می‌یابد.

با شناسایی اعضای شبکه بات می‌توان از بسیاری حملات جلوگیری کرد، البته کشف عضویت بات به صورت منفعل کار دشواری است. اغلب حمله کننده برای این‌که از کشف نشدن بات موجود در شبکه خود اطمینان حاصل کند، پرس‌وجوهایی را روانه DNS می‌نماید. و DNS، با توجه به لیست سیاهی که دارد پاسخ می‌دهد. این لیست سیاه را

DNSBL[۱] می‌نامند. (A ;.Ramachandran,۲۰۰۶:۱-۲) می‌باشد. این رویکرد به تحلیل منفعل ترافیک پرس‌وجوی DNSBL برای کشف شبکه‌های بات می‌پردازد. مشخصاتی که برای کشف می‌تواند مورد استفاده قرار بگیرد مبتنی بر مشخصات زمانی[۲] و فاصله‌ای[۳] موجود در پرس‌وجوی معتبر و قانونی می‌باشد.

- **روابط فاصله‌ای:** یک سرور پست الکترونیکی قانونی و مورد اعتماد، هم می‌پرسد (نرخ خروجی) و هم مورد پرسش قرار می‌گیرد (نرخ ورودی). اما میزبان‌هایی که پرس‌وجوهای غیرقانونی انجام می‌دهند تنها سوال می‌پرسند. به همین دلیل می‌توان با مقایسه نرخ ورود و نرخ خروج، میزبان‌های مشکوک را یافت.
- **روابط زمانی:** پرس‌وجوهای DNSBL یک سرور پست الکترونیک مورد اعتماد و قانونی، منعکس کننده‌ی الگوهای رسیدن پیغام‌های پست الکترونیک هستند. جستجوهای قانونی زمانی انجام می‌گیرند که پست‌های الکترونیکی به میل سرور می‌رسند و بنابراین نرخ پرس‌وجوها منعکس کننده‌ی نرخ‌های رسیدن پست‌های الکترونیک می‌باشند. اما پرس‌وجوهای غیرقانونی دارای چنین الگویی نیستند. در این رویکرد با ساخت یک درخت، تعداد دفعاتی که یک میزبان پرسش کرده است و یا مورد پرسش قرار گرفته است، محاسبه می‌گردد و میزبان‌های مشکوک کشف می‌شوند. از نتایج جالبی که در آزمایشات بدست آمد این بود که شبکه بات، پرس‌وجوهای DNSBL را بر روی نصف بات‌های دیگر شبکه‌های بات اجرا می‌کنند. همچنین می‌توان با تحت نظر داشتن پرس‌وجوهای انجام گرفته از بات‌های قدیمی به بات‌های جدید دست پیدا کرد.

نتیجه‌گیری

یکی از تهدیدات روزافزون در اینترنت و شبکه‌های کامپیوتری که اصل دسترس پذیری را نقض می‌کند، شبکه‌های بات می‌باشد. شبکه بات شبکه‌ای از کامپیوترهای آلوده متصل به اینترنت می‌باشد و برای حملات توزیع شده‌ی اینترنتی مانند ممانعت از سرویس، مورد استفاده قرار می‌گیرد.شبکه‌های بات به سرعت در حال پیشرفت هستند و از روش‌های جدیدی برای به دام انداختن کاربران و افزایش حفاظت از کامپیوترهای آلوده خود بهره می‌برند. همانطور که گفته شد حمله کنندگان برای دشوار کردن عمل ردگیری و کشف آن-

---

۱-DNS black list

۲-temporal

۳-spatial

ها به تکنولوژی‌های جدید همچون DNS و تغییرات پی‌درپی سریع روی آورده‌اند. یکی از انواع تغییرات پی‌درپی سریع، تغییرات پی‌درپی نام دامنه می‌باشد که در این نوع چندین نام دامنه به یک آدرس IP نگاشت داده می‌شود. در این پژوهش به معرفی مفاهیم مرتبط با شبکه‌های بات پرداخته و نحوه‌ی ایجاد و انتشار آن‌ها را شرح داده شد و با مروری بر تهدیدات به وجود آمده توسط این شبکه‌ها، روش‌های مقابله و کشف آن را بررسی گردید. در مراکز نظامی جهت مقابله با بات ها دو راه پیش روی کارشناسان امنیتی است.

راه اول؛ که امروزه در بسیاری مراکز، نهادها و سازمانها مرسوم است، محدود کردن دسترسی‌ها و قوانین محدودیت استفاده از تکنولوژیهای جدید است. ولی این راه حل به هیچوجه علمی و توجیه‌پذیر نبوده و به گونه‌ای پاک کردن صورت مسئله است.

راه دوم؛ برای مراکز نظامی تشکیل تیم‌های امنیتی قوی و تخصصی جهت رصد کردن بات‌ها و ابداع راه حل و تکنیک جهت مقابله با تهدیدات ناشی از آن‌ها می‌باشد.

می‌توان این‌گونه سخن را به پایان برد که بحث کشف و ردیابی شبکه‌های بات همچنان بحث جالب و چالش برانگیزی خواهد بود. زیرا همواره تکنیک‌ها و فناوری‌های جدیدی توسط حمله کننده‌ها به کار برده می‌شود که کار تشخیص ترافیک شبکه‌های بات را دشوار می‌سازد.

منابع

[۱] E. Passerini, *et al.*, "FluXOR : Detecting and Monitoring Fast-Flux Service Networks," in *Detection of Intrusions and Malware, and Vulnerability Assessment*. vol. ۵۱۳۷, D. Zamboni, Ed., ed: Springer Berlin / Heidelberg, ۲۰۰۸, pp. ۱۸۶-۲۰۶.

[۲] J. Nazario and T. Holz, "As the net churns: Fast-flux botnet observations," in *Malicious and Unwanted Software .۲۰۰۸ ,MALWARE ۲۰۰۸. ۳rd International Conference on*, ۲۰۰۸, pp. ۲۴-۳۱.

[۳] C. Brandhorst and A. Pras, "DNS: A Statistical Analysis of Name Server Traffic at Local Network-to-Internet Connections," in *EUNICE ۲۰۰۵: Networks and Applications Towards a Ubiquitously Connected World*. vol. ۱۹۶, C. Kloos, *et al.*, Eds., ed: Springer Boston, ۲۰۰۶ ,pp. ۲۵۵-۲۷۰.

[۴] http://www.securelist.com/en/analysis/۲۰۴۷۹۲۱۸۰/TDL۴_Top_Bot

[۵] J. Goebel and T. Holz, "Rishi: identify bot contaminated hosts by IRC nickname evaluation," resented at the Proceedings of the first conference on First Workshop on Hot Topics in Understanding Botnets, Cambridge, MA, ۲۰۰۷.

[۶] A. Ramachandran, *et al.*, "Revealing botnet membership using DNSBL counter-intelligence," presented at the Proceedings ofthe ۲nd conference on Steps to

Reducing Unwanted Traffic on the Internet - Volume ۲, San Jose, CA, ۲۰۰۶.

[۷] R. Villamarin-Salomon and J. C. Brustoloni, "Identifying Botnets Using Anomaly Detection Techniques Applied to DNS Traffic," in *Consumer Communications and Networking Conference, ۲۰۰۸. CCNC ۲۰۰۸. ۵th IEEE*, ۲۰۰۸, pp. ۴۷۶-۴۸۱.

[۸] C. Hyunsang, *et al.*, "Botnet Detection by Monitoring Group Activities inDNS Traffic," in *Computer and Information Technology, ۲۰۰۷. CIT ۲۰۰۷. ۷th IEEE International Conference on*, ۲۰۰۷, pp. ۷۱۵-۷۲۰.

[۹] M. Bailey, *et al.*, "A Survey of Botnet Technology and Defenses," in *Conference For Homeland Security, ۲۰۰۹. CATCH .۰۹' Cybersecurity Applications & Technology*, ۲۰۰۹, pp. ۲۹۹-۳۰۴.

[۱۰] G. Gu, *et al.*, "BotMiner: clustering analysis of networktraffic for protocol- and structure-independent botnet detection," presented at the Proceedings of the ۱۷th conference on Security symposium, San Jose, CA, ۲۰۰۸.

[۱۱] A. Caglayan, *et al.*, "Behavioral analysis of fast flux service networks," presented at the Proceedings of the ۵th Annual Workshop on Cyber Security and Information Intelligence Research: Cyber Security and Information Intelligence Challenges and Strategies, Oak Ridge, Tennessee, ۲۰۰۹.

[۱۲] A. Caglayan, *et al.*, "Real-Time Detection of Fast Flux Service Networks," in *Conference For Homeland Security, ۲۰۰۹. CATCH '۰۹. Cybersecurity Applications & Technology*, ۲۰۰۹, pp. ۲۸۵-۲۹۲.

[۱۳] K. Yuji, "Bot Detection Based on Traffic Analysis," in *The ۲۰۰۷ International Conference on Intelligent Pervasive Computing (IPC ۲۰۰۷)*, Jeju Island, Korea, ۲۰۰۷, pp. ۳۰۳-۳۰۶.

[۱۴] D. Dagon, *et al.*, "A taxonomy of botnets," in *Proceedings of CAIDA DNS-OARC Workshop*, San Jose, CA, ۲۰۰۵.

[۱۵] G. Ollmann, "Botnet communication topologies," *Damballa white paper*, ۲۰۰۹.

[۱۶] Samuel Greengard," The war against botnets", Magazine Communications of the ACM Volume ۵۵Issue ۲, February ۲۰۱۲

[۱۷]Manoj Rameshchandra Thakur۱, etal, "Detection and prevention of botnets and malware in an enterprise network", International Journal of Wireless and Mobile Computing Volume ۵, Number ۲/۲۰۱۲