بهبود روش تشخیص بات نت‌ها در کانال IRC

افسانه رستمی نجف آبادی[۱]، عبدالحسین رضائی[۲]، فرزین یغمائی[۳]

[۱] دانشجوی مهندسی کامپیوتر- نرم‌افزار کامپیوتر، دانشگاه جامع علمی کاربردی، مرکز آموزش عالی علمی کاربردی جهاددانشگاهی واحد سمنان
سمنان، ایران

a_rostami1389@yahoo.com

[۲] عضو هیات علمی جهاد دانشگاهی واحد صنعتی اصفهان و دانشجوی دکتری برق، دانشکده مهندسی برق و کامپیوتر دانشگاه سمنان
اصفهان، ایران

rezaie@acecr.ac.ir

[۳] عضو هیات علمی، دانشکده مهندسی برق و کامپیوتر، دانشگاه سمنان
سمنان، ایران

f_yaghmaee@semnan.ac.ir

چکیده

یکی از بزرگترین تهدیدات در فضای سایبری بات‌نت‌ها می‌باشند. در این مقاله یک روش جدید برای شناسائی بات‌نت و محل استقرار بات‌مستر در شبکه از طریق تجزیه و تحلیل رفتار بات‌ها ارائه شده است. در روش پیشنهادی از سه خصوصیت زیر برای تشخیص محدوده بات‌نت استفاده شده است: ۱) بات‌ها دارای تراکم غیر عادی در شبکه می‌باشند. ۲) بات‌ها در زمان دریافت فرمان از بات‌مستر ترافیک زیادی در شبکه ایجاد می‌کنند. ۳) زمان پاسخگویی آنها یکسان می‌باشد. با تشخیص محدوده بات‌نت از خصوصیات زیر برای شناسائی بات‌ها و بات‌مستر استفاده شده است: ابتدا اینکه کلیه فرمان‌ها در بات‌نت توسط بات‌مستر صادر می‌شود. ثانیاً آدرس مبدأ و مقصد از طریق سرآیند هر بسته ارسالی قابل پیگیری می‌باشد. لذا مبدأ اکثر بسته‌ها در بات‌نت، بات‌مستر و مقصد آن مربوط به بات می‌باشد. با استفاده از این خصوصیت بات‌مستر شناسائی شده و بات‌ها را می‌توان از کاربران قانونی تشخیص داد. نتایج نشان می‌دهد که روش پیشنهادی دارای کارائی بالاتری نسبت به سایر روش‌ها می‌باشد.

کلمات کلیدی:

دفاع سایبری، امنیت، بات‌نت، بات، سرور کنترل و فرمان (C&C)، ترافیک شبکه، کانال IRC

۱- مقدمه

در سال‌های اخیر گسترش کاربردهای اقتصادی، نظامی، سیاسی و ... از اینترنت نظیر تجارت الکترونیکی، ارسال نامه‌های محرمانه، بانکداری اینترنتی و ...، امنیت اطلاعات در فضای سایبری را به یکی از مهمترین مباحث تبدیل نموده است [۱، ۲، ۳]. یکی از جدی‌ترین و بزرگترین تهدیدات در فضای سایبری باتنت‌ها[1] می‌باشند[۱].

باتنت‌ها مجموعه‌ای از ماشین‌های آلوده (زومبی[2]) به نام بات[3] می‌باشند که بوسیله یک مرکز کنترل به نام باتمستر[4] برای انجام یک فعالیت مخرب و حملات سنگین کنترل می‌شوند [۱، ۴، ۵]. بعضی از باتنت‌ها شامل میلیون‌ها بات بوده و حملات سنگینی نظیر حمله DDOS[5] را در فضای سایبری انجام داده‌اند. از این‌رو تشخیص، تحلیل و خنثی کردن باتنت‌ها قبل از انجام فعالیت مخرب، دارای اهمیت بسیار زیادی است [۶، ۷].

برای تشخیص باتنت تلاش‌های زیادی انجام شده است. این تلاش‌ها را بطور کلی می‌توان به دو دسته تقسیم نمود: ۱) استفاده از تله ظرف عسل ۲) تجزیه و تحلیل ترافیک شبکه [۸، ۹]. هر چند برای استفاده از تله ظرف عسل تلاش‌های زیادی صورت گرفته است [۸، ۹، ۱۰، ۱۱]. اما این روش نمی‌تواند ماشین‌های آلوده (بات) را بطور کامل تشخیص دهد [۹]. در عوض استفاده از روش تجزیه و تحلیل ترافیک شبکه می‌تواند اطلاعات مفیدی در مورد باتنت ارائه نماید. تلاش‌های زیادی برای تشخیص باتنت از طریق تجزیه و تحلیل ترافیک شبکه صورت پذیرفته است از آن جمله می‌توان به جمع‌آوری اطلاعات مربوط به هرزنامه‌ها[6]ی ارسالی [۱۲]، پرس‌وجو از DNS[7] [۱۳، ۱۴]، پرس و جو از لیست سیاه DNS [۱۵]، تحلیل ترافیک شبکه در کانال IRC[8] [۶، ۱۶]، اندازه‌گیری زمان پاسخ‌گوئی کاربران [۶] و نحوهٔ توزیع کاربران [۶] اشاره نمود.

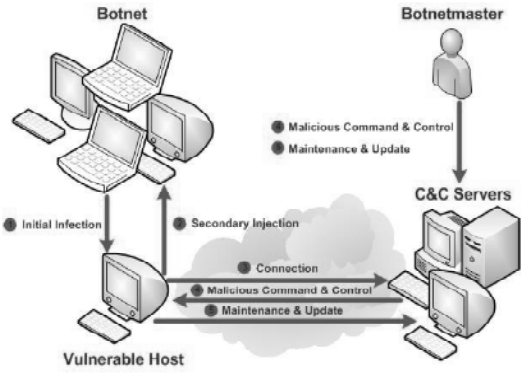
در [۶] از سه روش تحلیل ترافیک شبکه، اندازه‌گیری زمان پاسخ‌گوئی کاربران و نحوهٔ توزیع کاربران برای تشخیص محدوده باتنت‌ها استفاده شده است. ما در این مقاله براساس روش ارائه شده در [۶]، یک روش جدید برای شناسائی باتنت و محل استقرار باتمستر در شبکه از طریق تجزیه و تحلیل رفتار بات‌ها ارائه نموده‌ایم. در این روش ابتدا مشابه روش [۶]، با تجزیه و تحلیل ترافیک شبکه، ساختار توزیع کاربران و اندازه‌گیری زمان پاسخگوئی کاربران محدوده‌های مشکوک شناسائی می‌شود. علاوه بر این، در این مقاله با استفاده از آدرس مبدا و مقصد، کاربران قانونی از بات‌ها تشخیص داده شده و همچنین محل استقرار باتمستر شناسائی می‌شود. از این‌رو در روش پیشنهادی به جای محدوده مشکوک به باتنت، آدرس مربوط به باتمستر و بات‌ها (خود باتنت) قابل شناسائی می‌باشد.

در ادامه در بخش ۲ نحوه کار یک باتنت شرح داده شده است. توپولوژی‌های ارتباطی باتنت‌ها در بخش ۳ ارائه شده است. در بخش ۴ روش پیشنهادی برای تشخیص باتنت و باتمستر ارائه شده است. در بخش ۵ روش پیشنهادی مورد ارزیابی قرار گرفته است و بخش ۶ به جمع‌بندی اختصاص داده شده است.

۲- نحوهٔ کار یک باتنت

باتنت به مجموعه‌ای از کامپیوترهای آلوده به نام بات اطلاق می‌شود که بوسیله یک مرکز کنترل به نام باتمستر برای انجام یک فعالیت مخرب تحت پروتکل کنترل و فرمان[9] (C&C) کنترل می‌شود [۱،۴،۵]. در واقع بات‌ها، برنامه‌های نرم‌افزاری هستند که بر روی کامپیوترهای قربانی نصب می‌شوند و باتمستر را قادر می‌سازد که کامپیوترهای قربانی را از راه دور کنترل نماید [۷]. برای اجرای C&C سرویس‌های مختلفی ارائه شده است. سرویس IRC به دلیل سادگی برای پیاده‌سازی و ایجاد امکان کنترل در سطح بالا، مقبولیت بیشتری دارد [۱۴]. نحوهٔ ایجاد و کار یک بات در شکل ۱ نشان داده شده است.

[1] Botnets
[2] Zombie
[3] Bot
[4] Bot-master
[5] Distributed-Denial-Of-Service
[6] Spam
[7] Domain Name System
[8] Internet Relay Chat
[9] Command and control (C&C) protocol



شکل۱: نحوهٔ ایجاد و کار بات‌نت [۹]

همانگونه که در شکل ۱ نشان داده شده است ایجاد بات و انجام کار در یک بات‌نت شامل ۵ مرحله می‌باشد [۹]: ۱) آلودگی اولیه ۲) نفوذی ۳) اتصال ۴) فرمان و کنترل مخرب ۵) به روز رسانی. ابتدا مهاجم، بات را روی کامپیوترهای قربانی نصب می‌نمایند. سپس بات به بات‌مستر وصل شده تا دستورات لازم را دریافت نماید. بطور معمول این کار از طریق کانال IRC انجام می‌شود. سرور کنترل و فرمان (C&C) پس از دریافت درخواست بات، فرمان‌های لازم را برای بات از طریق کنترل کننده ارسال می‌نماید. سرانجام بات فرمان‌های را دریافت و اجرا می‌نماید.

۳- توپولوژی‌های ارتباطی بات‌نت‌ها

از لحاظ نحوهٔ ارتباط بات‌ها و بات‌مستر، بات‌نت‌ها را می‌توان به سه دسته تقسیم نمود: بات‌نت‌های متمرکز، بات‌نت‌های نامتمرکز و بات‌نت‌های ترکیبی. در ادامه این سه دسته بطور مختصر شرح داده می‌شوند [۴، ۶، ۸].

۳-۱- بات‌نت‌های متمرکز

در این نوع بات‌نت، یک نقطه مرکزی به نام بات‌مستر فرمان‌های لازم را به همهٔ بات‌ها ارسال می‌کند. تاخیر ارسال فرمان در این نوع بات‌نت بسیار کم می‌باشد و بات‌مستر به راحتی می‌تواند حمله را آغاز نماید. اما در این حالت احتمال شناسائی بات‌نت بخاطر اتصال تعداد زیادی بات به یک بات‌مستر زیاد می‌باشد [۶].

۳-۲- بات‌نت‌های نامتمرکز

در این نوع بات‌نت، از ایدهٔ ارتباط P2P[10] استفاده شده است. در این حالت بات‌مستر برای ارسال فرمان به تک‌تک بات‌ها وصل نمی‌شود بلکه بات‌ها نیز با هم در ارتباط می‌باشند. از این‌رو با تحلیل ترافیک شبکه در این نوع بات‌نت، بات‌مستر به راحتی قابل شناسائی نیست. اما در این نوع بات‌نت، هیچگونه تضمینی برای رسیدن فرمان به کلیه بات‌ها وجود ندارد. همچنین سرعت رسیدن فرمان به بات‌ها کم می‌باشد [۴].

۳-۳- بات‌نت‌های ترکیبی

این نوع بات‌نت، ترکیبی از چند بات‌نت متمرکز می‌باشند که خود با هم در ارتباط می‌باشند. در این حالت بات‌ها به دو گروه تقسیم می‌شوند: یک گروه که هم نقش سرور و هم نقش کلاینت را دارند و گروه دیگر که فقط نقش کلاینت را دارند. طراحی چنین بات‌نت‌هائی مشابه بات‌نت متمرکز ساده است. اما در این نوع بات‌نت، مشابه بات‌نت نامتمرکز هیچگونه تضمینی برای رسیدن فرمان به تمام بات‌ها وجود ندارد. همچنین تاخیر دریافت فرمان توسط بات در این نوع بات‌نت زیاد می‌باشد [۴].

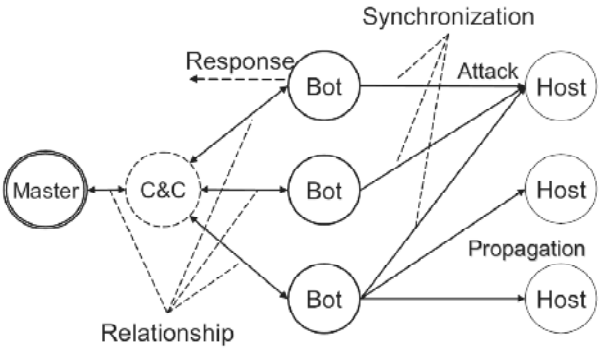
۴- روش پیشنهادی

امروزه بات‌نت‌های متمرکز بخاطر داشتن طراحی ساده، تاخیر بسیار کم در دریافت فرمان توسط بات و تضمین دریافت فرمان توسط بات مورد توجه قرار گرفته‌اند. از این‌رو در این مقاله یک روش جدید برای تشخیص بات‌نت، بات‌مستر و بات‌ها در بات‌نت‌های متمرکزی که از کانال IRC استفاده می‌کنند، ارائه شده است. دراین بخش ابتدا روش پیشنهادی برای تشخیص بات‌نت و سپس روش تشخیص بات‌مستر در بات‌نت‌های متمرکز ارائه شده است.

۴-۱- روش پیشنهادی برای تشخیص بات‌نت

همانگونه که در بخش ۲ بیان شد، همه فعالیت‌های مخرب بات‌ها براساس فرمان‌های بات‌مستر می‌باشد. نحوهٔ انجام یک فعالیت مخرب در یک بات‌نت در شکل ۲ نشان داده شده است.

[10] Peer to Peer



شکل۲: رفتار یک باتنت در زمان انجام فعالیت مخرب [۶]

با توجه به شکل ۲، رفتار باتنت‌ها از سه قاعده زیر پیروی می‌کنند: ارتباط، پاسخ و همزمانی [۶]. بنابراین برای شناسائی محدوده مشکوک به باتنت از سه روش زیر استفاده شده است:

۱) اندازه‌گیری ترافیک
۲) اندازه‌گیری زمان پاسخگویی کاربران
۳) بررسی تراکم کاربران.

در یک باتنت متمرکز، باتمستر با باتها یک رابطه یک به چندتایی دارد و تمام باتها بوسیله پروتکل کنترل و فرمان (C&C) و معمولاً از طریق کانال IRC به وسیلهٔ باتمستر هدایت می‌شوند در نتیجه تمام باتهای موجود در این نوع باتنت پس از دریافت فرمان باتمستر علاوه بر پاسخگویی دقیق و سریع بطور همزمان دستور یا دستورات دریافتی (فعالیت‌ها مخرب) را در زمان مقرر انجام می‌دهند. بنابراین در این بازه زمانی به دلیل فعالیت یکپارچه و همزمان باتها ترافیک بالایی در کانال IRC ایجاد می‌شود. لذا با اندازه‌گیری ترافیک شبکه و بررسی نقاط پر ترافیک، دامنه فعالیت باتها قابل تشخیص می‌باشد.

از طرفی باتها بعد از دریافت فرمان از باتمستر بصورت همزمان فعالیت مخرب خود را آغاز می‌نمایند، در نتیجه باعث بالا رفتن تراکم کلاینتها در کانال IRC می‌شوند. از این‌رو نقاطی که در زمان‌های خاص دارای تراکم بالایی هستند، می‌تواند نقاط مشکوک به حضور باتها باشد.

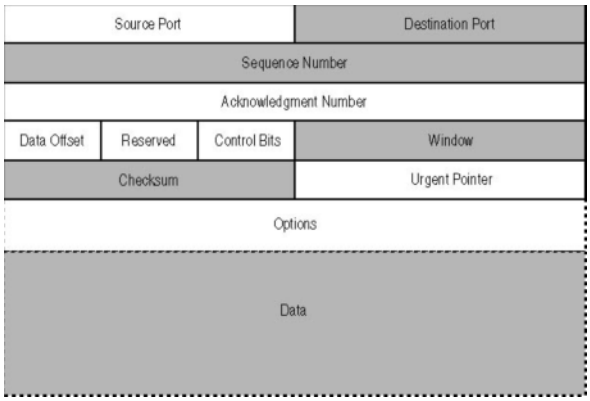
یکی دیگر از ویژگی رفتاری باتها زمان پاسخگویی آنها می‌باشد. درحالی که زمان پاسخگویی انسان‌ها به فرمان‌های مختلف، متفاوت می‌باشد، باتها به فرمان‌های مختلف در یک مدت زمان ثابت پاسخ می‌دهند. در نتیجه با اندازه‌گیری زمان پاسخگویی کاربران به فرمان‌های مختلف می‌توان باتها را از کاربران قانونی تشخیص داد.

از این‌رو با بررسی سه پارامتر فوق بطور همزمان می‌توان محدودهٔ مشکوک به باتنت را تشخیص داد.

۴-۲- روش پیشنهادی برای تشخیص باتمستر

بعد از تشخیص محدوده باتنت برای تشخیص باتها از کاربران قانونی و همچنین شناسائی باتمستر، ما به عنوان یک کاربر قانونی یا کامپیوتر قربانی به کانال IRC متصل شده و تمام بسته‌های موجود روی کانال IRC را در محدوده باتنت مانیتور می‌کنیم.

مطابق شکل۳ تمام بسته‌های ارسالی دارای فیلدهای سرآیندی هستند که در آن اطلاعاتی نظیر آدرس مبدا و آدرس مقصد وجود دارد[۱۷]. از این‌رو با بررسی سرآیند هر بسته می‌توان اطلاعات مربوط به آدرس‌های بسته‌های موجود روی کانال IRC را مشاهده نمود. با توجه به اینکه تمام باتها فرمان‌های خود را از یک نقطه به نام باتمستر دریافت می‌کنند (پروتکلC&C)، لذا با مقایسه آدرس‌های مبدا تمام بسته‌های موجود، می‌توان نتیجه گرفت که تعداد زیادی از بسته‌هایی که دارای آدرس مبدا یکسان هستند از طریق باتمستر برای باتها ارسال شده‌اند. از این‌رو آدرس مقصد موجود در این بسته‌های خاص آدرس باتهای موجود در کانال IRC می‌باشند و آدرس‌های مبدا این بسته‌ها آدرس باتمستر می‌باشد که با دنبال کردن این آدرس‌های مبدا و مقصد، می‌توان محل باتها و باتمستر را شناسایی کرد.



شکل۳: فیلدهای سرآیند بسته ارسالی

۵- ارزیابی طرح پیشنهادی

با توجه به اینکه در روش پیشنهادی ابتدا مشابه [۶]، به کمک بررسی ترافیک، زمان پاسخگویی و رفتار غیر عادی بات‌ها و بات‌مستر، نواحی مشکوک به بات‌نت شناسائی شده و سپس با استفاده از روش تشخیص آدرس مبدا ومقصد بات‌مستر و بات‌ها تشخیص داده می‌شوند. از این رو نسبت به روش ارائه شده در [۶] دارای دقت و کارایی بیشتری می‌باشد. زیرا در [۶] فقط محدوده بات‌نت شناسایی می‌شود.

با توجه به موارد فوق می‌توان نتیجه گرفت که کارائی روش پیشنهادی نسبت به روش‌های ارائه شده در [۶] بهبود یافته است.

۶- جمع‌بندی

در این مقاله با استفاده از روش‌های ارائه شده در [۶] یک روش جدید برای تشخیص بات‌نت و بات‌مستر ارائه شده است. در روش پیشنهادی از سه خصوصیت زیر برای تشخیص محدوده بات‌نت استفاده شده است: ۱) بات‌ها دارای تراکم غیر عادی در شبکه می‌باشند. ۲) بات‌ها در زمان دریافت فرمان از بات‌مستر ترافیک زیادی در شبکه ایجاد می‌کنند. ۳) زمان پاسخگویی آنها یکسان می‌باشد. با تشخیص محدوده بات‌نت از خصوصیات زیر برای شناسائی بات‌ها و بات‌مستر استفاده شده است: ۱) کلیه فرمان‌ها در بات‌نت توسط بات‌مستر صادر می‌شود. ۲) آدرس مبدا و مقصد از طریق سرآیند هر بسته ارسالی قابل پیگیری می‌باشد. لذا مبدا اکثر بسته‌ها در بات‌نت، بات‌مستر و مقصد آن مربوط به بات می‌باشد. با استفاده از این خصوصیت بات‌مستر شناسائی شده و بات‌ها را می‌توان از کاربران قانونی تشخیص داد.

بنابراین روش پیشنهادی نسبت به روش ارائه شده در [۶] دارای کارایی بیشتری می‌باشد. زیرا در [۶] فقط محدوده بات‌نت شناسایی می‌شود.

مراجع

[1] Stone-Gross, B., Cova M., Gilbert, B., Kemmerer, R., Kruegel, C. and Vigna, G., Analysis of a Botnet Takeover, IEEE. Security & Privacy, Vol.9, No.1, pp.64-72, 2011.

[2] Dogrul, M., Aslan, A., Celik, E., Developing an international cooperation on cyber defense and deterrence against cyber terrorism, proc. IEEE. Int. conf. on Cyber conflict, Tallinn, pp.1-15,2011.

[3] Rezai, A., Keshavarzi P. and Moravej, Z., A New Key Management Scheme for SCADA Networks, proc. abstract 2nd Int. Symp. on Computing in Science & Engineering, Kusadasi, Aydın, Turkey, pp. 373-378, 2011.

[4] Bailey, M., Cooke, E., Jahanian, F., Xu, Y. and Karir, M. A survey of botnet technology and defenses, proc. IEEE. Int. conf. on Cyber security Applications & Technology Conference for Homeland Security, Washington,DC, USA, pp. 299–304,. 2009.

[5] Geer, D., Malicious bots threaten network security, IEEE Computer January, Vol.38, No. 1, pp.18–20, 2005.

[6] Akiyama, M., Kawamoto, T., Shimamura, M., Yokoyama, T., Kadobayashi, Y., and Yamaguchi, S. A proposal of metrics for botnet detection based on its cooperative behavior, Proc. IEEE. Int. symp. on applications and the Internet Workshops(SAINT-W'07),Washington, DC, PP. 82-85, 2007.

[7] Stone-Gross, B., Cova, M., Cavallaro, L., Gilbert, B., Szydlowski, M., Kemmerer, R., Kruegel, C., and Vigna, G., Your Botnet is My Botnet: Analysis of a Botnet Takeover, proc. 16th ACM Int. conf. on Computer and Communication Security (CCS), Chicago, IL, USA, pp. 635-647, 2009.

[8] Zhu, Z., Lu, G., Chen, Y., Fu, Z., Roberts, P., Han, K., Botnet Research Survey, proc. 32nd Annual IEEE Int. conf. on Computer software and applications, Turku, Finland, pp.967- 972, 2008.

[9] Feily, M., Shahrestani, A., and Ramadass, S., A survey of botnet and botnet detection, proc. IEEE. Int. conf. on emerging security information, systems and technology Minden, Malaysia, pp. 268–273,. 2009.
[10] Dagon, D., Zou, C., and Lee, W., Modeling botnet propagation using time zones, in Proc. 13th Network and Distributed System Security Symposium (NDSS'06), 2006.
[11] Provos, N., A virtual honeypot framework, proc. 13th int. symp. on USENIX Security San Diego, CA, pp. 1–14, 2004,
[12] Zhuang, L., Dunagan, J., Simon, D., Wang, H., Osipkov, I., Hulten, G., and Tygar, J., Characterizing botnets from email spam records, proc. 1st ACM Usenix Workshop on Large-Scale Exploits and Emergent Threats, Berkeley, CA, USA, No.2, 2008.
[13] Rajab, M., Zarfoss, J., Monrose, F., and Terzis, A., My Botnet is Bigger than Yours (Maybe, Better than Yours) : Why Size Estimates Remain Challenging, proc. First ACM Workshop on Hot Topics in Understanding Botnets, Berkeley, CA, USA, pp. 5-5, 2007.
[14] Rajab, M., Zarfoss, J., Monrose, F., and Terzis, A., A Multifaceted Approach to Understanding the Botnet Phenomenon, proc. int. conf. on ACM Internet Measurement (IMC), New York, NY, USA , pp. 41 – 52, 2006.
[15] Ramachandran, A., Feamster, N., and Dagon, D., Revealing Botnet Membership Using DNSBL Counter-Intelligence, proc. Int. conf. on Steps to Reducing Unwanted Traffic on the Internet, Berkeley, CA, USA , pp.8-8, 2006.
[16] Karasaridis, A., Rexroad, B., and Hoeflin, D., Wide-scale botnet detection and characterization, proc. Int. ACM conf. on workshop on Hot Topics in Understanding Botnet, Berkeley, CA, USA , pp. 7-7, 2007.
[17] A. Tanenbaum, Computer Networks, Prentice Hall, Fourth Edition, 2002.