ارائه یک سیستم تحلیل ترافیک شبکه جهت شناسایی جریان‌های بات‌نتی

*افشین فیروزی[1]، مریم رحیمی‌پور[2] و دکتر شهرام جمالی[3]
[1]مدیر شبکه- مرکز فناوری اطلاعات و ارتباطات – اداره کل راه و شهرسازی استان اردبیل– firouzy.af@gmail.com
[2]گروه مهندسی کامپیوتر - دانشگاه آزاد اسلامی واحد علوم و تحقیقات اردبیل– rahimipour.m@gmail.com
[3]دانشیار- گروه مهندسی کامپیوتر و فناوری اطلاعات - دانشگاه محقق اردبیلی – ایران– jamali@iust.ac.ir

چکیده: بات‌نت[1] یکی از خطرات مهم ولی کمتر شناخته شده در اینترنت است. بات‌نت‌ها شبکه‌ای از کامپیوترهای تسخیر شده تحت کنترل هستند که از طریق یک کانال فرمان و کنترل[2] برای ترتیب دادن حملاتی با قدرت تخریب بالا و وسعت زیاد هدایت می‌شوند. بات‌نت‌ها اغلب برای اقدامات خرابکارانه مهمی همچون حملات انکار سرویس توزیع شده[3] مورد بهره-برداری قرار می‌گیرند. شناسایی ویژگی‌ها و شاخصه‌های اصلی بات‌نت‌ها در ایجاد و توسعه تکنولوژی‌های مواجهه با این خطر امنیتی مهم، موثر خواهد بود. در این مقاله بات‌نت‌ها، چرخه حیات آنها و انواع آن از نظر توپولوژی و پروتکل‌های مورد بهره‌گیری بررسی و با پیاده‌سازی یک شبکه آلوده به بات‌نت و ارائه سیستم آنالیز جریان شبکه، رفتارها و ویژگی-های ترافیک بات‌نتی مشاهده و مستند می‌شود. با پیاده‌سازی این سیستم ویژگی‌های جریان‌های بات‌نتی و رفتار بات‌نت به نحو مطلوبی نمایش داده شده است. مشاهده این ویژگی‌ها برای ارائه راهکارهای مقابله با حملات مبتنی بر بات‌نت موثر خواهد بود.

کلمات کلیدی: بات نت، جریان، حمله، فرمان و کنترل

1-مقدمه

امروزه بات‌نت به طور گسترده در حملات سایبری خطرناکی برای حمله به شبکه‌ها و دارایی‌های اطلاعاتی سازمان‌ها مورد استفاده قرار می‌گیرد. بات‌نت به بستر[4] اصلی و قابل توسعه‌ای برای حملات و اقدامات خرابکارانه تبدیل شده است و بیشتر انواع جدید حملات با استفاده از این بستر صورت می‌گیرد. بات‌ها جهت اجرای انواع گسترده‌ای از اقدامات مخرب و مجرمانه برعلیه سیستم‌ها و سرویس‌های آنها مورد استفاده قرار می‌گیرند. حملات DOS، انتشار اسپم[5]، فیشینگ و ... از جمله حملات قابل ترتیب توسط بات‌نت هستند[1]. بات‌نت یا شبکه بات از تعداد زیادی از کامپیوترهای آسیب‌پذیر که توسط کدهای مخربی[6] مورد نفوذ قرار گرفته‌اند و بوسیله فرمان‌های ارسالی از راه دور از طریق اینترنت تحت ساختار فرمان و کنترل قابل کنترل و هدایت هستند[2]. در ادامه در بخش دو در مورد ساختار بات‌نت بحث خواهد شد. چرخه حیات بات‌نت‌ها موضوعی است که در بخش سوم مطرح می‌شود. بخش چهارم در مورد معماری بات‌نت‌ها مواردی را مطرح می‌کند و در بخش پنجم پروتکل‌های ارتباطی بات‌نت‌ها معرفی و توضیح داده می‌شوند و پس از آن در بخش ششم مشخصه‌هایی از ترافیک و جریان بات‌نتی متمرکز که توسط سیستم ارائه شده مستند شده‌اند برای شناسایی آن از ترافیک نرمال معرفی خواهد شد و نهایتا در بخش آخر نتایج مقاله بررسی خواهند شد.

---
[1] Botnet
[2] Command and control
[3] Distributed denial of service
[4] Platform
[5] Spam
[6] Malicious code

2-ساختار باتنت

ساختار باتنت از سه قسمت عمده تشکیل شده است: بات، مدیر بات[۷]، کانال فرمان و کنترل.

کلمه بات از تلخیص ربات بدست آمده است که در برخی منابع به آن زامبی[۸] نیز گفته می‌شود. در واقع نوع جدیدی از بدافزارها[۹] است که بر روی کامپیوترهای آسیب پذیر از راه‌های مختلف و بهره‌گیری از مکانیزم‌های انتشار منتقل شده و امکان کنترل توسط نفوذگر که به آن مدیر بات می‌گویند را برای اجرای دستورات خاصی (معمولا خرابکارانه) فراهم می-آورد. پس از اینکه کد موردنظر بر روی کامپیوتر نصب شد کامپیوتر اشغال شده تبدیل به یک بات یا زامبی می‌شود. برخلاف سایر انواع بدافزارها مانند ویروس یا کرم[۱۰] که فعالیت اصلی آنها تمرکز بر روی میزبانی است که به آن نفوذ کرده اند، بات‌ها می‌توانند دستورات را از مدیر بات دریافت کرده و برای حمله به قربانی[۱۱] اصلی مورد استفاده قرار گیرند[3]. به اداره کننده بات و به عبارتی شخص یا گروهی از اشخاص که مدیریت و کنترل بات‌ها را از راه دور انجام می‌دهند، مدیر بات گفته می‌شود[3]. یکی از تفاوت‌های میان باتنت و ویروس در امکان کنترل آنها است[4]. باتنت از یک کانال فرمان و کنترل برای کنترل خود بهره می‌برد که بخش ضروری و اصلی شبکه بات همین ساختار فرمان و کنترل است و به اختصار به آن C&C گفته می‌شود. این زیرساخت شامل بات‌ها و یک یا چند موجودیت کنترل است که بسته به ساختار باتنت می‌تواند عمل کنترل را بصورت متمرکز یا توزیعی انجام دهد. زیرساخت C & C به طور معمول به عنوان تنها راه برای کنترل بات‌ها در باتنت عمل می‌کند. بات‌ها در این زیرساخت برای اجرای موثر و مناسب دستورات نیاز به ارتباطی پایدار دارند [2].

3-چرخه حیات باتنت

3-1- انتشار[۱۲]: باتنت می‌تواند در وسعت و ساختارهای مختلفی ایجاد شود اما همه آنها مراحل یکسانی را در چرخه حیات خود سپری می‌کنند. چرخه حیات باتنت پس از تولید کد دودویی مخرب با پروسه آلوده‌سازی سیستم‌های آسیب‌پذیر توسط انتشار فایل آلوده آغاز می‌شود. مدیر بات روش‌ها و تکنیک‌های مختلفی برای انتشار کد خود از طریق مکانیزم‌های انتشار در اختیار دارد. از جمله این تکنیک‌ها می‌توان به ایمیل‌های آلوده، بهره‌گیری از نرم‌افزارها و کرک‌ها اشاره کرد. پس از انتقال فایل دودویی به سیستم‌های آسیب‌پذیر و اجرای آنها، سیستم تبدیل به بات می‌شود[5].

3-2- ارتباطات[۱۳]: تفاوت عمده میان باتنت و سایر انواع بدافزارها وجود ارتباطات و بهره‌گیری از ساختار فرمان-کنترل (C&C) است. C&C اجازه دریافت فرامین و دستورات از مدیر بات را برای بات فراهم می‌کند[3]. به عبارت دیگر در مرحله ارتباطات، بات از طریق کانال در نظرگرفته شده برای فرمان و کنترل اقدام به برقراری ارتباط دوره‌ای با سرویس‌دهنده‌های فرمان و کنترل می‌کند. در این ارتباطات دستورات مورد نظر مدیر بات به بات منتقل می‌شود. به محض دریافت و شناسایی دستور جدید توسط بات، دستور دریافتی اجرا شده و نتایج اجرای آن به سرویس‌دهنده فرمان

---

[7] Botmaster
[8] Zombie
[9] Badware
[10] Worm
[11] Victim
[12] spreading
[13] Communications

و کنترل گزارش می‌شود و سپس بات منتظر دریافت دستورات جدید باقی می‌ماند. البته کانال ارتباطی صرفا برای برقرای ارتباط میان بات و مدیر بات به منظور دریافت فرامین نیست، ارتباطات می‌تواند برای اعلام زنده بودن بات یا دریافت نسخه‌های جدید به سرویس‌دهنده‌های فرمان- کنترل و یا حتی بین بات‌های یک بات‌نت برقرار شود. در هرصورت مدیر بات باید اطمینان حاصل کند که ساختار C&C برای مدیریت هزاران بات توزیع شده در سطح اینترنت به اندازه کافی قوی بوده و در مقابل تلاش‌هایی که برای شناسایی و ممانعت از برقراری ارتباطات صورت می‌گیرد عملکرد خوبی دارد.

3-3- حمله[۱۴]: هدف اصلی و نهایی یک بات‌نت اجرای یک حمله است. بات‌ها براساس فرامین دریافتی اقدام به حمله به هدف مشخص شده توسط مدیر بات می‌کنند. ویژگی اصلی حملات مبتنی بر بات‌نت تعداد زیاد حمله‌کنندگان و عملکرد گروهی و هماهنگ آنها در یک شبکه بات است. برخی اوقات پس از انجام یک حمله بات‌ها اقدام به برقرای ارتباط با سرویس‌دهنده‌های خاصی کرده و پس از بروزرسانی برای حملات دیگری سازماندهی می‌شوند[1]. بات‌نت ها عمدتا برای اجرای اقدامات خرابکارانه بر روی شبکه‌های کامپیوتری ایجاد می‌شوند[6] درواقع بات‌نت یک حمله نیست بلکه ساختاری برای اجرای انواع مختلف و در عین حال خطرناک حملات بر روی شبکه‌های کامپیوتری و اینترنت است [7]. با برخی از این حملات در ادامه آشنا می‌شویم:

3-3-1- حملات انکار سرویس نوعی از حملات هستند که در آن از ارائه یک سرویس جلوگیری بعمل آمده و آن را از دسترس خارج می‌کند. حملات انکار سرویس توزیع شده نوع خاصی از حملات انکار سرویس هستند که در آن چندین عامل حمله‌کننده به طور همزمان و هماهنگ و با هدف از کار انداختن و از دسترس خارج نمودن سرویس اقدام به حمله می‌کنند بنابراین ساختار بات‌نت‌ها برای ترتیب‌دادن این نوع از حملات کاملا مناسب است[1]. با توجه به کنترل بات‌ها، مدیر بات می‌تواند با ارسال یک دستور خاص به بات‌ها، اجرای آن دستور و حمله DOS را از هزاران نقطه مختلف در سراسر اینترنت از بات‌ها بخواهند[8،9].

3-3-2- هرزنگاری[۱۵] به پیام‌های ناخواسته‌ای که در حجم بسیار زیادی از طریق رسانه‌های مختلفی مانند ایمیل، نرم افزارهای گفتگوی نوشتاری، ارسال نظر در وبلاگ‌ها یا وب‌سایت‌ها و گروه‌های خبری ارسال می‌شوند گفته می‌شود [10]. براساس گزارش Kaspersky هشتادوپنج درصد از فعالیت‌های هرزنگاری توسط بات‌نت صورت می‌گیرد [11] بنابراین ساختار بات‌نت می‌تواند به عنوان بستر اصلی جمع‌آوری و ساماندهی آدرس‌های ایمیل از کامپیوترهای به اشغال درآمده توسط بات‌نت و ارسال هرزنامه مورد استفاده قرار گیرد. براساس بررسی‌های بعمل آمده، هر بات به طور میانگین می‌تواند در هر ثانیه 3 ایمیل یا پیام جعلی یا هرزنامه ارسال کند[12].

3-3-3- بات‌نت‌ها همچنین برای سرقت هویت[۱۶] و اطلاعات استفاده از آنها در جهت منافع مدیران بات مورد استفاده قرار می‌گیرند. بات‌ها می‌توانند به گونه‌ای برنامه‌ریزی شوند که اطلاعات مهم و مشخص موجود در وب‌سایت‌ها را مورد کاوش قرار دهند[7]. علاوه بر آن نرم‌افزارهای دیگری مانند گزارش‌گر کلیدها[۱۷] توسط بات‌ها برای ثبت و گزارش اطلاعات مهمی مانند کلمات عبور و یا اطلاعات تجاری مانند خدمات بانکی برخط به مدیران بات منتشر می‌شوند[13،12].

---

[14] Attack
[15] Spam
[16] Identity theft
[17] Keylogger

3-3-4- خدمات میزبانی، فروش و اجاره غیرقانونی: یک کامپیوتر یا سرور با فضای ذخیره‌سازی و اتصال با پهنای باند بالا بر روی اینترنت می‌تواند به عنوان یک هدف برای مدیر بات قرار گیرد تا با بدست گرفتن کنترل آن و استفاده برای خدماتی نظیر اشتراک فایل و میزبانی البته بصورت غیرقانونی مورد استفاده قرار دهد[12]. برنامه‌های باتنت و سرویس-های میزبانی برای فروش و یا اجاره برای دوره‌های معین موردنیاز جهت اهداف و مقاصد مجرمانه همواره در دسترس است. دلیل تمایل به این سرویس‌ها وجود موانع و فاصله بیشتر مابین خریداران و اجرای قانون است به عبارت بهتر امکان شناسایی حمله‌کننده اصلی که از این ساختار بهره می‌برد وجود ندارد[10،14].

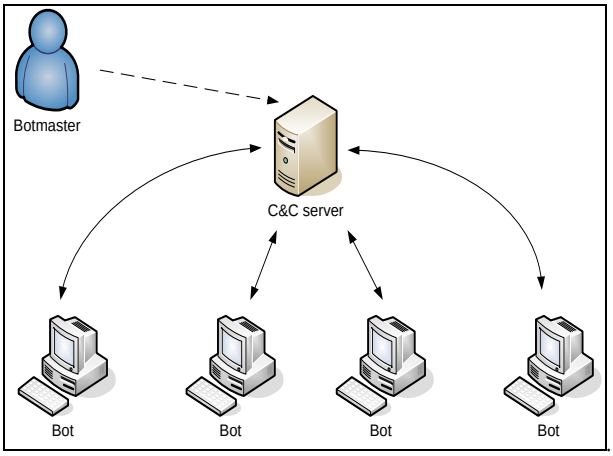
3-3-5- تبلیغ افزارها[18]: یکی دیگر از تفاوت‌های باتنت با سایر حملات و خطرات اینترنتی این است که باتنت‌ها می‌توانند برای صاحبان خود درآمد نیز تولید کنند. مدیران باتنت با استفاده از بات‌ها و بهره‌گیری از مزایای مالی بازدید از وب سایت‌هایی که این سرویس‌ها را ارائه می‌کنند درآمد هنگفتی عاید خود نمایند. ابزارهای تبلیغاتی نیز می‌توانند بر روی بات‌ها نصب شده و کاربران را مجبور به بازدید از صفحات خاصی از وب‌سایت‌ها کنند[10]. علاوه بر حملات مورد بحث، باتنت‌ها می‌توانند برای گسترش انواع مختلف از تهدیدها در قالب ویروس‌ها، تروجان‌ها، درب پشتی، کرم‌ها و ... مورد استفاده قرار گیرند[12].

4-معماری باتنت‌ها

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

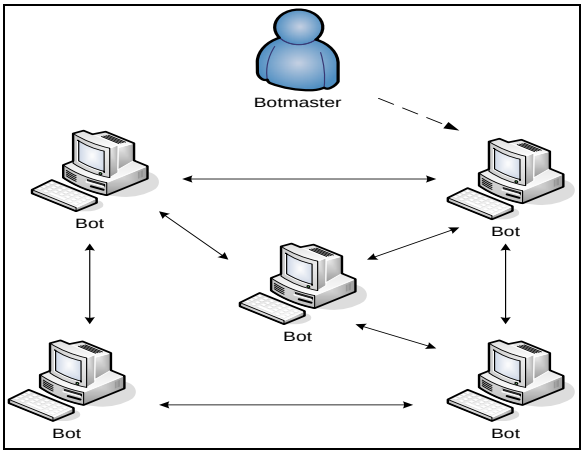
4-1- معماری متمرکز[19]: در معماری متمرکز فرمان و کنترل یک یا چند سرویس‌دهنده وظیفه مدیریت ارتباطات را برعهده دارند در واقع مشخصه اصلی این معماری وجود یک یا چند نقطه مرکزی برای مدیریت ارتباطات است. مدیر بات یک میزبان را را برای ارسال فرمان‌ها و کنترل بات‌ها در نظر می‌گیرد. این میزبان می‌توان یکی از کامپیوترهای آسیب-پذیر و اشغال‌شده توسط مدیر بات باشد و یا یک سرویس‌دهنده قانونی که خدمات مربوط به سرویس‌دهی اینترنتی را انجام می‌دهد. زمانی که بات به کد دودویی آلوده شد اقدام به برقراری ارتباط با سرویس‌دهنده کرده و منتظر دریافت فرامین و تنظیمات موردنظر مدیر بات می‌ماند[5]. در شکل 1 معماری ساختار متمرکز فرمان و کنترل نشان داده شده است. مزیت این معماری امکان پیاده‌سازی سریع و مدیریت آسان بات‌ها و باتنت نقطه ضعف عمده آن این است که با حذف سرویس‌دهنده فرمان و کنترل کل باتنت از بین خواهد رفت[12].

[18] Adware
[19] Centralized



شکل1: معماری ساختار متمرکز فرمان-کنترل

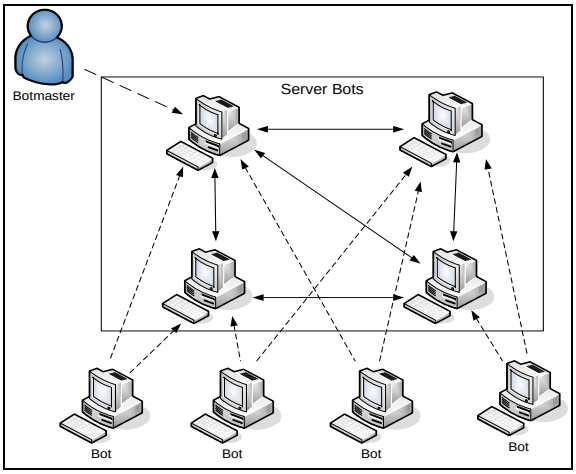
4-2- معماری غیرمتمرکز[20]: در معماری غیرمتمرکز فرمان-کنترل مدیر بات فرامین و تنظیمات را از چند نقطه بصورت غیرمتمرکز به بات‌ها ارسال می‌کند. ارتباطات بات‌ها و اعلام زنده بودن آنها نیز از طریق یک سرویس‌دهنده صورت نمی‌گیرد. بات‌ها تحت یک توپولوژی تصادفی و غیرمتمرکز فرمان و کنترل اقدام به برقراری ارتباطات خود می-کنند. در این معماری هر بات می‌تواند به عنوان سرویس‌دهنده فرمان و کنترل نیز عمل کند بنابراین دستورات از طریق یک بات به بات دیگر نیز منتقل می‌شود در این دستورات معمولا به بات گفته می‌شود که دستورات را میان عامل‌های دیگر گسترش دهد[3]. پیاده‌سازی این ساختار و مدیریت آن پیچیده‌تر از مدل متمرکز است اما مشکل نقطه یگانه شکست توپولوژی متمرکز در این روش حل شده است و با شناسایی و حذف یک سرویس‌دهنده فرمان و کنترل، کل باتنت از بین نمی‌رود[12]. شکل 2 معماری غیرمتمرکز فرمان و کنترل را نمایش می‌دهد.



شکل2: معماری غیرمتمرکز فرمان و کنترل

4-3- مدل ترکیبی[21]: همانگونه که شرح داده شد هر یک از معماری‌های متمرکز و غیرمتمرکز فرمان و کنترل با توجه به ساختار خود، مزایا و معایبی را به همراه داشتند. هدف از ایجاد معماری ترکیبی فرمان و کنترل بهره‌گیری از مزایا و کاهش دادن نقاط ضعف دو توپولوژی قبلی بصورت همزمان بوده است. این رویکرد ترکیبی از دو ساختار متمرکز و غیرمتمرکز است. معماری ترکیبی فرمان و کنترل در شکل 3 نمایش داده شده است.

[20] Decentralized
[21] Hybrid



شکل 3: معماری ترکیبی فرمان و کنترل

5- پروتکل[22]های ارتباطی بات‌نت

بات‌نت‌ها معمولا از پروتکل‌های ارتباطی شناخته شده برای ارتباطات خود استفاده می‌کنند. در [16] پروتکل‌های ارتباطی بات‌نت‌ها در سه گروه مختلف معرفی دسته‌بندی شده‌اند.

5-1- پروتکل IRC[23]: یکی از رایج‌ترین پروتکل‌ها برای ارتباط با بات‌ها که توسط مدیر بات مورد استفاده قرار می‌گیرد پروتکل IRC است. پروتکل IRC عموما برای ارتباطات یک به چند طراحی شده است اما می‌توان از آن برای ارتباطات یک به یک که برای کنترل بات‌نت بسیار مناسب است، نیز بهره برد. پیکربندی ابزارها و سیستم‌های امنیتی برای بلوکه کردن ترافیک مربوط به پروتکل IRC به سادگی صورت می‌گیرد.

5-2- پروتکل HTTP[24]: یکی دیگر از پروتکل‌های مورد استفاده بات‌نت‌ها که از محبوبیت زیادی نیز برخوردار است پروتکل HTTP است. بات‌نت‌هایی که از پروتکل HTTP استفاده می‌کنند به سختی قابل شناسایی هستند. بات‌نت‌ها از طریق این پروتکل قادر به دور زدن سیستم‌های تأمین امنیت شبکه هستند. امتیاز و ویژگی استفاده از این پروتکل این است که ترافیک بات‌نتی در میان ترافیک نرمال وب مخفی می‌شود و امکان فریب فایروالها و مکانیزم‌های کنترل پورت IDSها را فراهم می‌آورد.

5-3- پروتکل P2P[25]: اخیرا بات‌نت‌های پیشرفته و هوشمند از پروتکل دیگری به نام P2P در ارتباطات خود بهره می‌برند[17].

6- شناسایی جریان‌های بات‌نتی با ارائه یک سیستم مانیتورینگ ترافیک شبکه

6-1- محیط پیاده‌سازی: در این بخش ضمن بررسی مشخصات جریان‌های بات‌نتی نتایج مشاهدات حاصل از پیاده‌سازی یک شبکه آلوده به بات‌نت و سیستم تحلیل جریان مستند شده است. برای پیاده‌سازی شبکه آلوده به بات از بات‌نت معروف Zeus و تحلیل جریان از یک سرویس‌دهنده ISA[26] به همراه بانک اطلاعاتی SQL Server و زبان برنامه‌نویسی PHP و همچنین سرویس‌دهنده Apache بهره برده‌ایم. اطلاعات ترافیک شبکه از طریق سرویس‌دهنده ISA به

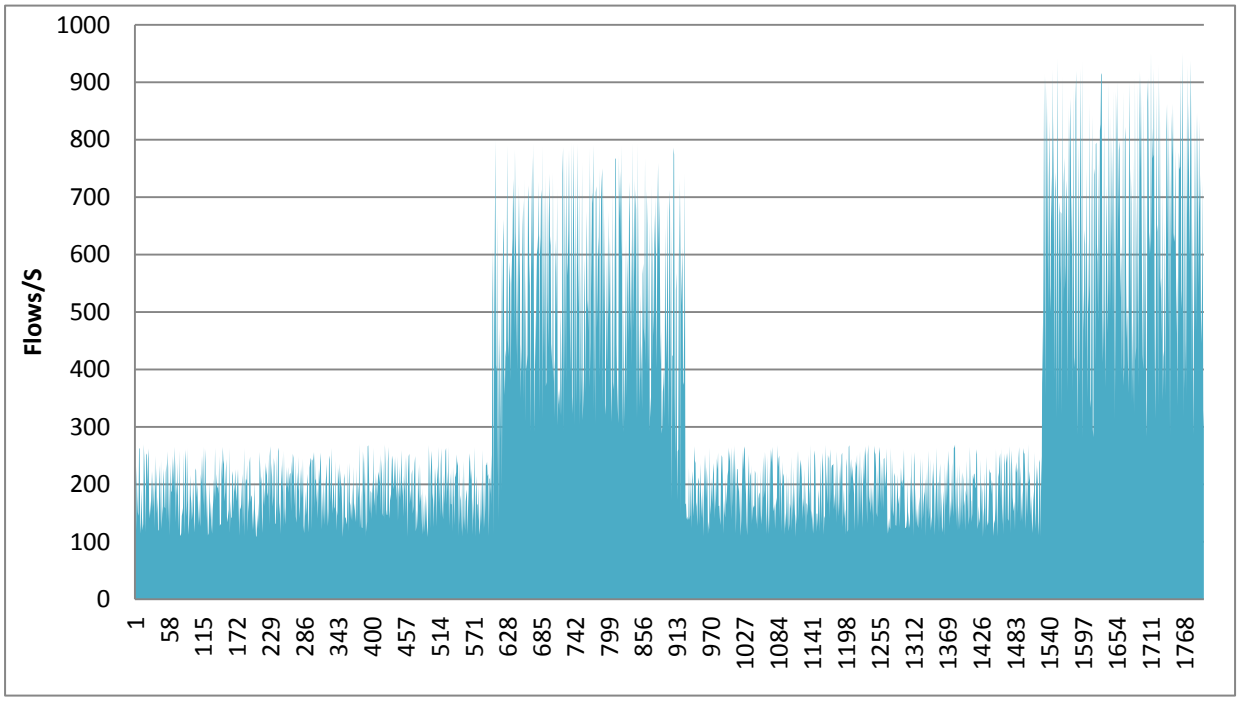
[22] Protocol
[23] Internet Relay Chat
[24] Hypertext Transfer Protocol
[25] Peer to Peer
[26] Internet Security and Acceleration Server

بانک اطلاعاتی SQL هدایت و در جداولی برای تحلیل ذخیره شده‌اند. ابـزار مانیتورینـگ شـبکه Wireshark نیـز جهـت مشاهده اطلاعات جریان‌ها مورد استفاده قرار گرفته است.

سناریو مورد نظر در یک شبکه با 30 کامپیوتر که 12 کامپیوتر در آن به عنوان بـات، یـک سـرویس‌دهنـده فرمـان و کنترل خارج از شبکه مذکور و یک مدیر بات که از طریق سیستم‌های دیگر امکان دسترسی تحت وب جهـت مـدیریت و کنترل بات‌ها را در اختیار داشت پیاده‌سازی گردید. تمام جریان‌های شبکه از طریق سرویس‌دهنده ISA به مقصد هدایت شده‌اند.

6-2- بررسی مشاهدات رفتار بات‌نت‌ها

6-2-1- افزایش ترافیک شبکه[۲۷]: با توجه به مانیتورینگ وضعیت ترافیک شبکه در طول آزمایشات مشاهده شـد کـه در مرحله ارتباطات و فرمان- کنترل از چرخه حیات بات‌نت‌ها سرویس‌دهنده فرمان و کنترل و بات‌ها ارتباطات منظمی با یکدیگر برقرار می‌کنند. این ارتباطات حجم ترافیک شبکه را بالا می‌برد[18,19]. شکل 4 افزایش میزان ترافیک شبکه را در طول مدت برقراری ارتباطات نشان می‌دهد.

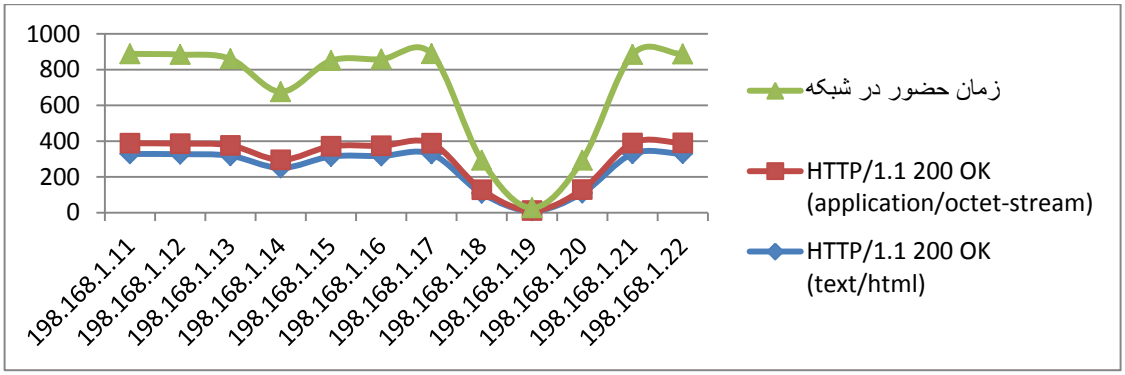


شکل 4: افزایش ترافیک شبکه در طول دوره‌های فرمان و کنترل

6-2-2- رفتار و درخواست‌های مشابه[۲۸] بات‌ها: بات‌های عضو یک گروه معمولا درخواست‌ها و رفتارهـای مشـابهی در شبکه از خود نشان می‌دهند[20]. با توجه به تحلیل نتایج صورت گرفته توسط سیستم ارائه شده مشاهده شد با توجه به عضویت بات‌ها در یک گروه، درخواست‌های مشابهی از سوی آنها ارسال می‌شود. آمار این درخواسـت‌هـای مشـابه معمـولا بالا و تقریبا برای تمام بات‌هایی که مدت زمان مشابهی در شبکه حضور داشته‌اند یکسان است. شکل 5 این موضوع را بـه خوبی نشان داده است. بات‌ها با آدرس 11 و12و 13و 15و 16 و 17 و 21و 22 با توجه به اینکه مدت زمان یکسانی در

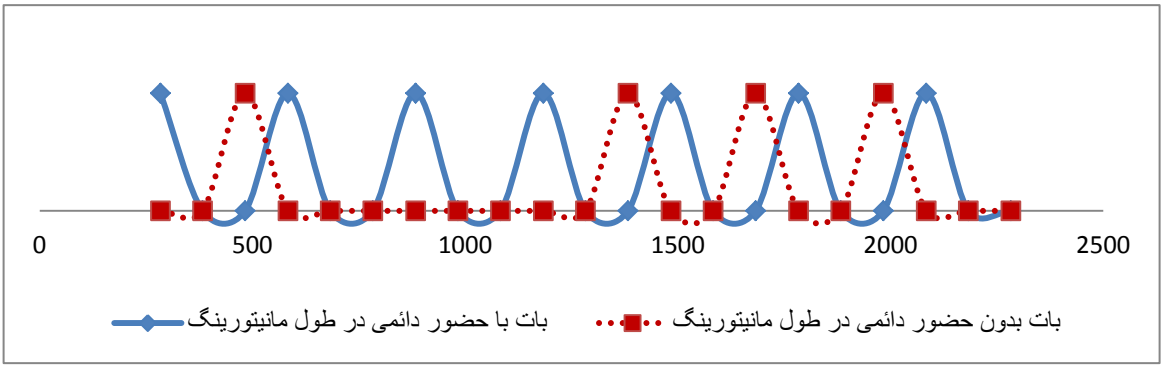
[27] Network traffic
[28] Similar requests

شبکه حضور داشته‌اند تقریبا دارای تعداد یکسانی از درخواست‌های مشابه ارسالی به سرویس‌دهنده فرمان و کنترل هستند.



شکل 5: میزان درخواست‌های ارسالی سیستم‌های آلوده به سرویس‌دهنده فرمان و کنترل

6-2-3- ارتباطات دوره‌ای[29] بات با سرویس‌دهنده فرمان و کنترل: با توجه به برنامه‌های از پیش تعیین شده برای بات‌ها، آنها در دوره‌های زمانی منظمی با سرویس‌دهنده فرمان و کنترل ارتباط برقرار کرده و ضمن اعلام زنده بودن، تنظیمات و فرامین مدیر بات را دریافت می‌کنند. نتیجه این ارتباطات یک رفتار منظم و دوره‌ای میان سرویس‌دهنده C&Cو بات می‌باشد. در انواع مختلف شبکه‌های بات در دوره‌های زمانی منظمی این ارتباطات برقرار می‌شود[21]. البته ممکن است به دلایل مختلفی مانند خاموش بودن سیستم یا قطع بودن ارتباط شبکه بات و به طور کلی عدم حضور بات در شبکه این رفتار دوره‌ای کامل نشود. شکل 6 درخواست‌های یکسان دو بات در یک دوره زمانی را نمایش می‌دهد. نقاط آبی در رأس سهمی‌ها زمان‌های برقراری ارتباط توسط سیستم آلوده‌ای را نمایش می‌دهند که در کل دوره مانیتورینگ در شبکه حضور داشته است. با اتصال نقاط آبی به یکدیگر یک نمودار هارمونیک و منظم بوجود می‌آید این نمودار موید برقراری ارتباطات در فواصل زمانی منظم میان بات و سرویس‌دهنده فرمان- کنترل است. نقاط قرمز در رأس سهمی‌های موجود در شکل 6 نیز مربوط به زمان‌های ارتباط باتی است که عمدا ارتباط آن با شبکه قطع شده است. با اتصال نقاط قرمز به یکدیگر عدم وجود هارمونی در زمان‌های ارتباط این بات کاملا مشهود شده است.



شکل6: نمودار Time Stamp ***برقراری ارتباط بات با سرویس‌دهنده C&C***

6-2-4- زمان پاسخگویی[30] کوتاه و اجرای سریع فرامین: بات‌ها معمولا بلافاصله پس از دریافت دستورات مدیر بات به آن پاسخ می‌دهد. این زمان پاسخگویی نسبت به زمان پاسخگویی بشر بسیار کمتر است. علاوه بر زمان پاسخگویی کوتاه ،

[29] Periodically communications
[30] Response time

بات دستورات مشخص مدیر بات را بلافاصله اجرا می‌کند[22]. سیستم ارائه شده با بررسی عکس العمل بات‌ها پس از دریافت فرامین از مدیر بات زمان پاسخگویی و اجرای فرامین توسط بات را به طور متوسط کمتر از 1ms ارزیابی کرده است.

6-2-5- اندازه کوچک دستورات[31]: طول بسته‌ها در ترافیک نرمال وب در حالت عادی نسبتا بزرگ است. به منظور جلوگیری از افزایش بار سرویس‌دهنده بات‌نت‌ها تمایل به دستورات با حجم بسته‌ای کوچک دارند[18]. طول بسته‌ها و دستورات مدیر بات که جهت اجرا به بات ارسال می‌شود معمولا 1KB و حتی کمتر از آن است[22]. با بررسی دستورات ارسالی به بات‌ها این موضوع کاملا مشخص و آشکار گردید.

مخفی ماندن ترافیک بات‌نت: با توجه به اینکه بات‌نت از پروتکل‌های استاندارد شبکه برای ارتباطات خود استفاده می‌کنند فعالیت آنها در میان ترافیک نرمال وب مخفی مانده و توسط سیستم‌های امنیتی و فایروال‌های مورد شناسایی قرار نمی‌گیرند با توجه به اینکه پروتکل HTTP برخلاف پروتکل‌های IRC و P2P برای ارائه گستره وسیعی از خدمات و سرویس‌های اینترنتی مورد استفاده قرار گرفته است نمی‌توان به راحتی این پروتکل و سرویس‌های آن را کنار گذاشت[23,12]. در شبکه مورد آزمایش نیز مخفی ماندن ترافیک بات‌نتی در میان ترافیک نرمال موجبات عدم شناسایی توسط سیستم‌های امنیتی را باعث گردید.

7-نتیجه‌گیری

بات‌نت به عنوان یکی از فراگیرترین و مخربترین حملات در اینترنت، یکی از جذاب‌ترین زمینه‌های فعالیت و تحقیق برای پژوهشگران امنیت شبکه به حساب می‌آید. شناخت و درک ساختار، نحوه عمل و ویژگی‌های مختلف بات‌نت منجر به تعریف استراتژی‌ها و راه حل‌های کشف و مقابله با بات‌نت خواهد شد. در این مقاله با پیاده‌سازی یک شبکه آلوده به بات و ارائه سیستم مانیتورینگ و تحلیل ترافیک شبکه آنالیزی از بات‌نت‌ها و جریان بات‌نتی توسط مانیتورینگ جریان با دو هدف ارائه شد: 1- شناسایی ساختار و چرخه حیات بات‌نت، انواع بات‌نت از نظر توپولوژی و پروتکل مورد استفاده 2- تمرکز بر روی جریان‌های بات‌نتی و رفتار بات‌نت و برجسته کردن ویژگی‌های آن جهت بهره‌گیری در الگوریتم‌های تشخیص و مقابله با بات‌نت.

8-تشکر و قدردانی

برخود لازم می‌دانیم مراتب سپاس خود را به مدیریت محترم، فناوری اطلاعات و ارتباطات و واحد تحقیقات و ارتباط با دانشگاه اداره کل راه و شهرسازی استان اردبیل که زمینه پیاده‌سازی و انجام آزمایشات مربوط به پروژه را برای ما فراهم نمودند، تقدیم نماییم.

مراجع:

[1] Rodrıguez-Gómez, R. A., Maciá-Fernández, G., & Garcıa-Teodoro, P. (2011). Analysis of Botnets through life-cycle. In SECRYPT 2011-International Conference on Security and Cryptography.

[2] Upadhyaya, A., Jayaswal, D., & Yadav, S. (2011, April). Botnet: A new network terminology. In Emerging Trends in Networks and Computer Communications (ETNCC), 2011 International Conference on (pp. 424-428). IEEE.

[3] Zeidanloo, H. R., & Manaf, A. A. (2009, December). Botnet command and control mechanisms. In Computer and Electrical Engineering, 2009. ICCEE'09. Second International Conference on (Vol. 1, pp. 564-568). IEEE.

[31] Little command size

[4] Cai, T., & Zou, F. (2012, September). Detecting HTTP Botnet with Clustering Network Traffic. In Wireless Communications, Networking and Mobile Computing (WiCOM), 2012 8th International Conference on (pp. 1-7). IEEE.
[5] Hachem, N., Ben Mustapha, Y., Granadillo, G. G., & Debar, H. (2011, May). Botnets: lifecycle and taxonomy. In Network and Information Systems Security (SAR-SSI), 2011 Conference on (pp. 1-8). IEEE.
[6] N. Hachem, Y. Ben Mustapha, G. G. Granadillo, and H. Debar, "Botnets: Lifecycle and Taxonomy," in Proceedings of the Conference on Network and Information Systems Security (SAR-SSI), 2011, pp. 1-8.
[7] M. Chandramohan and H. Tan, "Detection of Mobile Malware in the Wild," Computer, vol. 45, pp. 65-71, 2012.
[8] L. Chao, J. Wei, and Z. Xin, "Botnet: Survey and Case Study," in Proceedings of the Fourth International Conference on Innovative Computing, Information and Control (ICICIC), 2009, pp. 1184-187.
[9] E. Yuce, "A Literature Survey About Recent Botnet Trends," GÉANT Network, ULAKBIM,Turkey, Rep. JRA2 T4, 2012.
[10] C. Elliott, "Botnets: To What Extent Are They a Threat to Information Security?," Information Security Technical Report, vol. 15, pp. 79-103, 2010.
[11] V. Kamluk. (2009). The Botnet Ecosystem [Online]. Available: http://www.securelist.com/en/analysis/204792095/The_Botnet_ecosystem
[12] Eslahi, M., Salleh, R., & Anuar, N. B. (2012, November). Bots and Botnets: An overview of characteristics, detection and challenges. In Control System, Computing and Engineering (ICCSCE), 2012 IEEE International Conference on (pp. 349-354). IEEE.
[13] B. Stone-Gross, M. Cova, B. Gilbert, R. Kemmerer, C. Kruegel, and G. Vigna, "Analysis of a Botnet Takeover," Security & Privacy, IEEE, vol.
[14] Cisco, "Cisco 2009 Midyear Security Report: An Update on Global Security Threats and Trends," Cisco Systems, Rep., 2009.
[15] M. Bailey, E. Cooke, F. Jahanian, X. Yunjing, and M. Karir, "A Survey of Botnet Technology and Defenses," in Proceedings of the Cybersecurity Applications & Technology Conference for Homeland Security (CATCH), 2009, pp. 299-304.
[16] Taxonomy of Botnet Threats. Trend Micro Inc. White Paper,November, 2006.
[17] J. B. Grizzard, V. Sharma, C. Nunnery, B. B. Kang, and D. Dagon."Peer-to-peer Botnets: Overview and case study," In Proc. of ot Topics in Understanding Botnets (HotBots'07), 2007:198~201.
[18] Cai, T., & Zou, F. (2012, September). Detecting HTTP Botnet with Clustering Network Traffic. In Wireless Communications, Networking and Mobile Computing (WiCOM), 2012 8th International Conference on (pp. 1-7). IEEE.
[19] Chen, C. M., Ou, Y. H., & Tsai, Y. C. (2010, December). Web Botnet detection based on flow information. In Computer Symposium (ICS), 2010 International (pp. 381-384). IEEE.
[20] Arshad, S., Abbaspour, M., Kharrazi, M., & Sanatkar, H. (2011, December). An anomaly-based Botnet detection approach for identifying stealthy Botnets. In Computer Applications and Industrial Electronics (ICCAIE), 2011 IEEE International Conference on (pp. 564-569). IEEE.
[21] AsSadhan, B., Moura, J. M., & Lapsley, D. (2009, November). Periodic behavior in Botnet command and control channels traffic. In Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE (pp. 1-6). IEEE.
[22] M. M. Masud, T. Al-khateeb, L. Khan, B. Thuraisingham and K. W. Hamlen, "Flow-based identification of Botnet traffic by mining multiple log files," in Proc. DFmA 2008, 2008.
[23] K. Tung-Ming, C. Hung-Chang, and W. Guo-Quan, "Construction P2P Firewall HTTP-Botnet Defense Mechanism," in Proceedings of the IEEE International Conference on Computer Science and Automation Engineering (CSAE), 2011, pp. 33-39.