دانشکده مهندسی کامپیوتر

مطالعه‌ای بر روی روش‌های تشخیص بات‌نت‌ها

پژوهش درس مهندسی نرم‌افزار پیشرفته

دانشجویان:

محسن امیریان – مرتضی ذاکری – سعید امیری

استاد درس:

دکتر پارسا

خرداد ۱۳۹۶

چکیده

تشـــخیص باتنت نقش مهمی را در امنیت شـــبکه بازی می‌کند. باتنت مجموعه‌ای از کامپیوترهای در معرض خطر هســت که اصــطلاحا بات نامیده می‌شــوند. برای تشــخیص حضــور بات‌ها در یک شــبکه فنون مختلفی وجود دارد. روش تشخیص مبتنی بر شبکه یکی از روش‌های کارآمد در تشخیص بات‌ها است. این گزارش چند فن مختلف را معرفی کرده و آن‌ها را با یکدیگر مقایسه می‌کند.

کلمات کلیدی: بات؛ باتنت؛ سرویس دهنده‌ی مرکز کنترل و فرمان؛ سرویس دهنده‌ی IRC

فهرست مطالب

عنوان **صفحه**

۱- شناسایی بات‌نت‌ها ۱

۱ـ۱ـ معرفی ۱

۱ـ۲ـ چرخه حیات بات‌نت ۲

۱ـ۳ـ طبقه بندی روش‌های موجود در شناسایی باتنت‌ها ۳

۱ـ۴ـ معرفی روش‌های شناسایی ۳

۱ـ۴ـ۱ـ روش‌های مبتنی بر امضا ۳

۱ـ۴ـ۲ـ روش‌های مبتنی بر ناهنجاری ۴

۱ـ۴ـ۳ـ روش‌های مبتنی بر میزبان ۴

۱ـ۴ـ۴ـ کشف بات‌نت بر اساس وضعیت شبکه ۴

۱ـ۴ـ۵ـ روش‌های مبتنی بر DNS ۵

۱ـ۴ـ۶ـ روش‌های مبتنی بر داده کاوی ۵

۱ـ۵ـ بحث و نتیجه گیری ۵

۱ـ۶ـ جمع بندی ۶

شناسایی بات‌نت‌ها

۱-۱- معرفی

اینترنت به طور مکرر توسط انواع متنوعی از حملات نظیر ویروس‌ها، کرم‌ها و غیره تهدید می‌شود. این حمله‌ها تأثیرات منفی روی شبکه دارد که نتیجه آن ازدحام شبکه، اتلاف پهنای باند شبکه و همچنین فساد و خرابی کامپیوترها و داده‌های کاربران است. افزون بر آن، بعضی از این حمله‌ها برای به کنترل گرفتن میزبان‌های اینترنتی و سپس استفاده از این میزبان‌ها برای انجام حمله ممانعت از سرویس (DoS) روی دیگر بخش‌ها انجام می‌شود. اگر حمله‌کننده بتواند به میزبان‌های شبکه دسترسی پیدا کند، این امر می‌تواند منجر به آسیب‌های سنگینی نظیر مختل کردن وب سایت‌های تجارت الکترونیکی، رسانه‌های خبری، زیر ساخت شبکه، مسیریاب‌ها و سرورهای نام دامنه شود.

در زندگی مدرن، بدافزار، نرم‌افزار مخربی است که موقعیت مهمی را گرفتار می‌کند. از ابتدای عصر سیستم‌های قابل برنامه‌ریزی، فنون آلوده سازی این قبیل سیستم‌ها، با نرم‌افزاری‌هایی که حاوی کد مخرب هستند، وجود داشته است؛ اما، در گذشته بدافزارها فقط تأثیر محدود یا محلی داشتند. موفقیت شبکه‌های کامپیوتری، نقطه آغازی برای گزارش آسیب‌های مخربی که میلیون‌ها سیستم را در سراسر دنیا تحت تأثیر قرار می‌دهند، شد. بنابراین هدایت از راه دور شبکه‌ای از کامپیوترهای ربوده شده، که بات‌نت نامیده شد،

محبوب شده است. باتنت مجموعه‌ای از سیستم‌های کامپیوتری در معرض خطر و قابل هدایت یا کنترل از راه دور است. مهمترین هدف باتنت‌ها شامل توزیع هرزنامه‌ها، حمله‌های ممانعت از سرویس توزیع شده (DDoS)، توزیع بدافزارها و غیره است.

باتنت ترکیب دو واژه «ربات» و «کار» است. بات‌ها ماشین‌های آسیب‌پذیری هستند که با اجرای کد مخرب یا دودویی بات، آلوده می شوند. وقتی که یک بات آلوده شد، تلاش می‌کند تا سرویس‌دهنده کنترل و فرمان خود را پیدا و به آن متصل شود. سرویس‌دهنده C & C سرویس‌دهنده کنترل و فرمان است که یک کانال ارتباطی را برای ارتباط بین بات‌ها و رئیس اصلی آن‌ها فراهم می‌کند. بات‌هایی توسط یک رئیس کنترل می‌شوند، botmaster یا botherder نامیده می‌شوند. مهمترین هدف باتنت انجام فعالیت‌های مخرب در پشت سرویس‌دهنده‌اش به منظور ایجاد سود است؛ زیرا، بات‌ها ارزان هستند و انتشار آنها آسان است. معماری ارتباطی باتنت یک جنبه کلیدی در باتنت‌ها است. بات‌ها بر روی یک کانال قانونی ارتباط برقرار می‌کنند.

برای شناسایی حضور باتنت‌ها و برای غلبه بر اثرات منفی آنها بر روی شبکه، فنون تشخیص باتنت بسیاری وجود دارند. تشخیص مبتنی بر شبکه یکی از روش‌های کارآمد در تشخیص بات‌ها است. فنون دیگر تشخیص باتنت‌ها که در اینجا مورد بررسی قرار گرفته‌اند فنون مبتنی بر امضا، فنون مبتنی بر بی‌نظمی و فنون مبتنی بر میزبان هستند.

۲-۱- چرخه حیات باتنت

چرخه حیات باتنت پنج مرحله مختلف را شامل می شود. به منظور اینکه یک ماشین آسیب‌پذیر، به یک بات فعال تبدیل شود و یک قسمت از باتنت باشد، ماشین یک چرخه از مراحل را طی می‌کند.

مرحله اول مرحله آغاز آلودگی نامیده می شود. در این مرحله ماشین آلوده شده و پتانسیل بات شدن را پیدا می‌کند. ماشین با دریافت ناخواسته بدافزار از یک وب سایت یا استفاده از یک حافظه قابل حمل آلوده و غیره، آلوده می‌شود.

مرحله دوم دومین مرحله تزریق ثانویه است. در اینجا میزبان آلوده برنامه‌ای را اجرا می‌کند که فایل دودویی بات را در پایگاه‌داده شبکه جست‌جو می‌کند. هر زمان ماشین فایل دودویی باتنت را دریافت و آن را اجرا کرد، آن ماشین شروع به رفتار کردن شبیه به یک بات واقعی خواهد نمود.

مرحله سوم مرحله اتصال یا تجمع است؛ جایی که بات تلاش می‌کند تا به مرکز کنترل و فرمان خود متصل شود. وقتی بات به این مرکز متصل شد، می‌تواند فرمان‌های botmaster را دریافت و به آنها پاسخ دهد. این مرحله چندین مرتبه در چرخه حیات بات رخ می‌دهد. بات در طول این مرحله آسیب‌پذیر می‌شود.

مرحله چهارم مرحله تخریب است؛ یعنی جایی که بات تلاش می‌کند مجموعه‌ای از فعالیت‌های مخرب را بر اساس آن دستوراتی که از botmaster خود دریافت نموده است، صورت دهد. بات می‌تواند چندین حمله

تخریب‌کننده را انجام دهد؛ از جمله حمله ارسال هرزنامه، حمله ممانعت از سرویس توزیع شده، توزیع و پخش نرم‌افزارهای مخرب و غیره.

مرحله پنجم و نهایی مرحله نگهداری و ارتقا است. botmaster تلاش می‌کند تا بات خود را تا حد امکان تحت کنترل خود قرار دهد. نگهداری به منظور بروز نگهداشتن botmaster به همراه ارتش بات‌های تحت کنترل خود مورد نیاز است تا فعالیت‌های آتی بات‌ها را هماهنگ نماید. در این مرحله بات رفتار خود را بروزرسانی نموده و فعالیت‌های مخرب جدیدی را بر اساس آن اطلاعاتی که از botmaster خود دریافت نموده، صورت می‌دهد.

۱-۳- طبقه بندی روش‌های موجود در شناسایی بات‌نت‌ها

حمله‌ی بات نت ها در قالب یک گروه برای انجام جرایم سایبری انجام می‌گیرد. این امر بسیار خطرناک بوده و می‌توانند منجر به خرابی هر نوع شبکه، سرویس دهنده، سازمان، و یا به طور کلی اینترنت شوند.

بنابراین می‌باید کارهای سخت بسیاری صورت گیرد تا زیان‌های اقتصادی و صدمه‌های وارده بر تشکیلات شبکه و داده‌ها را که باعث و بانی آن‌ها بات نت‌ها هستند، به حداقل برسانیم. این کار با شناسایی بات نت ها دقیقاً پس از شکل گیری آن‌ها امکان پذیر است.

جهت تشخیص و درک اینکه بات نت ها چگونه کار می‌کنند، مطالعات بسیاری انجام شده است. در گذ شته تنظیم و نصب honeypot ها بر روی اینترنت جهت کمک به د ستگیری بد افزارها و درک رفتار بات نت ها، مرسوم بوده است. تکنولوژی بات نت ها و مشخصات آن ها با کمک honeypot ها قابل فهمیدن است، اما لزوما منجر به کشف خرابی های آن نمی‌شود.

روش‌های تشخیص بات نت‌ها براساس نظارت بر شبکه، بسیار مفید هستند. همچنین شیوه‌های شناسایی دیگری نیز وجود دارند که عبارت است از: روش‌های مبتنی بر امضا[1]، روش‌های مبتنی بر ناهنجاری[2]، روش‌های مبتنی بر DNS، روش‌های مبتنی بر داده کاوی و روش‌های مبتنی بر میزبان[3].

۱-۴- معرفی روش‌های شناسایی

۱-۴-۱- روش‌های مبتنی بر امضا

این روش‌ها برای شناسایی انواع شناخته شده بات نت‌ها استفاده می شوند. این روش‌ها امضای بات‌های

1 Signature-Based

2 Anomaly-Based

3 Host-Based

موجود (شناخته شده) را به یک سیستم شناسایی IDS اعمال می‌کنند. امضا به الگویی گفته می شود که درون یک بسته‌ی شبکه مشاهده می‌گردد. به کمک پایگاه داده‌ی امضاها، اعمال شناسایی بات‌ها با مقایسه کردن هر بایت درون بسته، انجام می‌گیرد.

ضعف این روش در ناتوانی در شناسایی بات‌های ناشناخته است. همچنین می‌بایست داعماً پایگاه داده‌ی امضاها را به روز رسانی کرد.

۱-۴-۲- روش‌های مبتنی بر ناهنجاری

این روش‌ها تلاش می‌کنند بات نت ها را بر اساس برخی از ناهنجاری‌های موجود در ترافیک شبکه شناسایی کنند. مانند حجم بالای ترافیک شبکه، تاخیر زیاد شبکه، ترافیک بر روی پورت‌های غیر معمول و رفتار غیرمعمول سیستم همگی نشان دهنده‌ی احتمال وجود بات نت در شبکه هستند.

این روش از رفتار شبکه برای شناسایی بات‌ها استفاده می‌کند. ناهنجاری‌ها به رفتارهای غیرمنتظره در شبکه اطلاق می‌شود که متفاوت با رفتار عادی شبکه هستند. مقایسه ای بین رفتار فعلی و رفتار قبلی شبکه صورت می‌گیرد. رفتار جدید شبکه یا پذیرفته شود و یا به عنوان یک ناهنجاری شناخته شده که می‌بایست در قبال آن اقدامات بعدی صورت گیرد. برای درک رفتار شبکه می‌توان از موتور IDS استفاده کرد که رفتار عادی و قابل انتظار سیستم را مدل کرده و ممکن است انحراف از این رفتارِ قابل انتظار را شناسایی کند که این انحراف ممکن است نشان دهنده‌ی یک نقص امنیتی و یا تلاش برای یک حمله باشد.

ضمناً برخی از بات‌های ناشناخته را می‌توان با بررسی سرآیند[۱] بسته‌های شبکه شناسایی کرد.

۱-۴-۳- روش‌های مبتنی بر میزبان

این روش‌ها به دنبال نشانه‌هایی از رفتار های بات مانند در کامپیوترهای میزبان هستند.

یکی از روش‌ها، شناسایی کامپیوتر آلوده با زیر نظر گرفتن رویدادها و جزئیات فایروال برای تعیین عملیات بات، می‌با شد. همچنین برای شناسایی مکان بات، برخی از روش ها از بررسیِ راه اندازی[۲] بدخواه پردازه‌ها، استفاده می‌کنند.

۱-۴-۴- کشف بات نت بر اساس وضعیت شبکه

کشف باتنت بر اساس وضعیت ترافیک شبکه، از تکنیک های تشخیص مبتنی بر شبکه است. در این روش، ترافیک های شبکه برای کشف باتنت ها تجزیه و تحلیل می‌شوند. روش تجزیه و تحلیل وضعیت ترافیک می‌تواند بر روی کانال های رمزگذاری شده نیز بکار گرفته شود. اگر بات هایی در شبکه وجود داشته

---

۱ Header

۲ Start Up

با شند، خاموش کردن سرور IRC مناسب ترین اقدام برای ممانعت از باتنت ها است. در شبکه، بات نت ها بوسیله ی تقسیم شدن (شکسته شده) به پنجره های زمانی مختلف، مورد بررسی قرار می گیرند. سپس از هر پنجره ی زمانی، مجموعه ای از ویژگی ها استخراج می شود که برای دسته بندی ترافیک ها از نظر بدخواه بودن یا نبودن مورد استفاده هستند. بات ها تشابهاتی در ترافیک هایشان نشان می دهند که در تشخیص آنها از ترافیک های معمولی کمک کننده است. از ویژگی های مشترکی که توسط بات در یک بات نت ارائه می شود، یکنواختی در رفتار ترافیکی، رفتار ارتباطی و غیره است. ایده ی کلی در این زمینه این است که امضایی یکتا در رفتارِ جریان برای هر یک بات واحد وجود دارد. این امضا می تواند برای تشخیص بات ها در یک بات نت مشابه مورد استفاده قرار گیرد. این تکنیک برای الگوریتم های رمزنگاری استفاده شده و از روش های دیگر کم هزینه تر است. این تکنیک قادر به کشف سریع فعالیت بات بواسطه ی تقسیم کردن (شکستن) جریان های منحصر بفردِ آن به پنجره های زمانی مختلف است.

۱-۴-۵- روش‌های مبتنی بر DNS

این روش‌ها از اطلاعات DNS بات نت استفاده می‌کنند. بات‌ها برای یافتن مرکز کنترل و فرمان خود، پرس و جو های DNS انجام می‌دهند. در این روش با کمک ترافیک DNS، بات ها قابل شناسایی خواهند بود.

۱-۴-۶- روش‌های مبتنی بر داده کاوی

روش‌های داده کاوی برای استخراج، تجزیه و تحلیل، تشخیص و کشف الگوهای طبیعی و غیرطبیعی در حجم بسیار زیاد داده‌ها استفاده می‌شوند.

در ارتباط با موضوع شناسایی بات نت ها، روش‌های یادگیری ماشین[۱]، طبقه بندی[۲]، خوشه بندی[۳] و... همگی روش‌های داده کاوی هستند که استفاده می‌شوند.

۱-۵- بحث و نتیجه گیری

در این گزارش چندین تکنیک متفاوت برای کشف باتنت بیان گردید. مقایسه چهار تکنیک اول در جدول ۱-۱ ارائه شده است. روش‌های تشخیص مبنتی بر امضا بطور عمده بر امضای بات‌ها، تنها برای

۱ Machine Learning
۲ Classification
۳ Clustering

شناخـت باتها مفیـد اسـت، تمـرکز دارند. روش‌های مبنتـی بر ناهنجاری، اختـلالات را در ترافیک شبکه تشخیص می‌دهد. رفتارهای غیرطبیعی در کشف باتها کمک می‌کنند. اما زمانیکه ترافیک شبکه رمز شده باشد این روش قابل استفاده نیست؛ در حالیکه که امروزه اکثر باتنت ها از کانال‌های رمز شده برای ارتباطات استفاده می‌کنند، شناسایی رفتار میزبان اصل کلی برای روش‌های مبنتی بر میزبان است.

روش‌های مبنتی بر میزبان به تشخیص کارآمدتر، نسبت به روش‌های مبتنی بر امضا و مبتنی ناهنجاری، کمک می‌کند اما سـربار پردازشـی بسـیار زیادی نیز دارد. در روش‌های مبنتی بر شـبکه، فعالیت‌های بات مستقیما و با توجه به جریان‌های شبکه مشخص می‌شود. این مورد به کشف باتها و در مراحل اولیه‌ی توسعه و گسترش آنها کمک می‌کند. این روش بر مشکل موجود در روش‌های مبتنی بر امضا، بدلیل کشف باتها با دقت بالا فائق آماده است. اما زمانیکه از محتوای بسته برای مقاصد بدخواهانه استفاده شده باشد، این روش کارآمد نخواهد بود چرا که در این روش محتوای بسته‌ها مورد بررسی قرار نمی‌گیرند.

جدول (۱ـ۱) مقایسه روش‌های شناسایی باتنت‌ها

معایب	مزایا	ویژگی	تکنیک
عدم کشف بات‌های ناشناخته	کشف بات‌های شناخته شده	تشخیص بر اساس امضای بات	مبتنی بر امضا
عدم توانایی در بررسی کانال‌های رمز شده	تجزیه و تحلیل چندین ترافیک شبکه بی‌نظم	شناسایی رفتارهای غیرطبیعی شبکه	مبتنی بر ناهنجاری
سربار محاسباتی	ارائه میزان پایینی از نرخ مثبت کاذب	جستجو برای رفتارهای شبه بات در میزبان	مبتنی بر میزبان
عدم بررسی محتوای بسته‌های شبکه	شخیص باتها در مراحل اولیه‌ی توسعه آنها کشف بات‌های ناشناخته	مانیتور کردن جریان شبکه برای یافتن فعالیت باتها	مبتنی بر شبکه

۱-۶- جمع بندی

چندین تکنیک متفاوت کشف باتنت برای یافتن بـدافزار در این گزارش ذکر شـد. با اینکه تکنـیک‌های مختلفی برای کشف بات‌های حاضر در شبکه وجود دارد، روش مبتنی بر شبکه متداول‌تر است. این روش هم

بات‌های شناخته شده و هم ناشناخته را شناسایی می‌کند. این فرآیند تشخیص زمانی دچار چالش می‌شود که بات‌نت ها معماری مرکز کنترل و فرمان را تغییر دهند؛ اما چالش اصلی در کشف بات‌نت دشواری در آزمودن روش‌های تشخیص با اطلاعات جهان واقعی است.