
بسم الله الرحمن الرحيم

سمینار

عنوان

مطالعه و ارزیابی تشخیص بات‌نت‌ها

نگارنده:

فهرست مطالب

عنوان **صفحه**

چکیده..... ٦

فصل اول: مقدمه ٧

١-١- مقدمه ٨

فصل دوم: مروری بر باتنت‌ها ١٠

٢-١- مقدمه ١١

٢-٢- معرفی بات‌ها..... ١٣

٢-٣- مطالعه توپولوژی بات‌نت‌ها..... ١٤

٢-٤- انواع باتنت‌ها..... ١٩

٢-٤-١- باتنت‌های متمرکز ١٩

٢-٤-١-١- باتنت مبتنی بر IRC..... ١٩

٢-٤-١-٢- باتنت مبتنی بر HTTP..... ٢٠

٢-٤-٢- باتنت غیرمتمرکز..... ٢٠

٢-٤-٢-١- باتنت نظیر به نظیر..... ٢١

٢-٤-٢-٢- باتنت‌های ترکیبی ٢٢

٢-٥- چرخه حیات باتنت‌ها..... ٢٣

٢-٦- مرحله شکل‌گیری..... ٢٤

٢-٦-١- مکانیزم‌های انتشار..... ٢٤

٢-٦-٢- مکانیزم‌های الحاق..... ٢٤

٢-٦-٣- مکانیزم‌های ساخت هم‌بندی..... ٢٦

٢-٦-٤- مرحله فرمان و کنترل..... ٢٧

٢-٦-٥- مرحله حمله..... ٢٨

٢-٧- انواع باتنت ها از نظر مکانیزم مورد استفاده برای انتشار و آلوده‌سازی..... ٢٨

٢-٨- مقایسه باتنت‌های مبتنی بر سرور و مبتنی بر کلاینت..... ٢٩

٢-١١- جمع‌بندی..... ٣١

فصل سوم: مطالعه و بررسی روش‌های تشخیص باتنت **۳۲**

۳-۱- مقدمه ۳۳

۳-۲- معیارهای طبقه‌بندی روش‌های تشخیص باتنت ۳٤

۳-۲-۱- تشخیص در مراحل آغازین ۳۵

۳-۲-۲- تشخیص در مرحله حمله ۳۷

۳-۳- روش‌های تشخیص باتنت ۳۸

۳-۳-۱- Honeypot ۳۹

۳-۳-۲- سیستم‌های تشخیص نفوذ ٤۰

۳-۳-۳- روش‌های بیولوژیکی ٤۵

۳-۳-٤- کشف بلادرنگ باتنت‌ها ٤۷

۳-٤- مقایسه روش‌ها تشخیص باتنت‌ها ٤۹

۳-۵- تشخیص باتنت‌ها با مانیتور کردن ترافیک DNS ۵۰

۳-۵-۱- ویژگی‌های درخواست های ایجاد شده توسط باتنت‌ها در DNS ۵۱

۳-۵-۲- الگوریتم تشخیص درخواست‌های ایجاد شده توسط باتنت‌ها ۵۳

۳-۵-۳- الگوریتم تشخیص مهاجرت ۵٦

۳-۳- جمع بندی ۵۷

فصل چهارم: نتیجه گیری و پیشنهادات **۵۸**

٤-۱- نتیجه گیری و پیشنهادات ۵۹

مراجع **٦۱**

فهرست اشکال

شکل ۲-۱- رشد قربانیان باتنت‌ها در طی سال ۲۰۱۰ میلادی ۱۲
شکل ۲-۲- عناصر باتنت ۱۳
شکل ۲-۳- توپولوژی‌های متفاوت باتنت‌ها ۱۵
شکل ۲-٤- تعداد نشریات باتنت‌ها در هر سال ۱۸
شکل ۲-۵- نمایی از یک باتنت با ساختار متمرکز مبتنی بر IRC ۲۰
شکل ۲-٦- نمایی ازیک باتنت با ساختار غیرمتمرکز نظیر به نظیر ۲۲
شکل ۲-۷- نمایی از یک بات نت با ساختار غیرمتمرکز ترکیبی ۲۳
شکل ۲-۸- چرخه حیات باتنت ۲۳
شکل ۳-۱- طبقه‌بندی روش‌های تشخیص باتنت براساس سه معیار مرحله تشخیص ۳۵
شکل ۳-۲- شباهت و همبستگی مکانی- زمانی در پاسخ بات‌ها ۳۸
شکل ۳-۳- نحوه وارد کردن درخواست‌های DNS ۵۳
شکل ۳-٤- الگوریتم وارد کردن درخواست‌های DNS ۵٤
شکل ۳-۵- الگوریتم حذف درخواست‌ها قانونی ۵۵
شکل ۳-٦- الگوریتم تشخیص درخواست‌های بات‌ها ۵۵

فهرست جداول

جدول ۲-۱- توپولوژی باتنت‌ها تا به امروز ۱۶
جدول ۲-۲- روند توسعه و تکامل باتنت‌ها در طول زمان ۱۷
جدول ۲-۳- جدول مقایسه باتنت-های مبتنی بر سرور و باتنت‌های مبتنی بر کلاینت ۳۰
جدول ۳-۱- دسته‌بندی نقاط قوت و ضعف روش‌های کشف باتنت‌ها ٤۹
جدول ۳-۲- مقایسه روش-های مختلف ۵۰
جدول ٤-۱- تفاوت‌های ترافیک قانونی و ترافیک باتنت ۵۲

چکیده

سال‌های اخیر حملات سایبری شکل جدید به خود گرفته است و با پیشرفت علم و تکنولوژی، ابزارهای جدیدی برای اینگونه حملات بوجود آمده است. باتنت‌ها در واقع نمونه‌ای از این ابزارهای جدید می‌باشند که باعث می‌شوند حملات سایبری با قدرت مضاعفی اجرا شوند. بنابراین، باتنت‌ها امروزه به جنگ افزاری قدرتمند در جنگ سایبری تبدیل شده‌اند. آگاهی از انواع باتنت و پارامترهای مختلف آنها ما را در نبرد پیش می‌اندازد. باتنت به گروهی از ماشین‌های آلوده در سطح شبکه گفته می‌شود که از راه دور توسط یک هکر کنترل می‌شوند. امروزه انواع متفاوتی از روش‌های تشخیص بانت وجود دارند که هر کدام از آنها براساس پروتکل‌ها و توپولوژی‌های خاص باتنت‌ها کار می‌کنند. هدف تمامی این روش‌ها این است که باتنت‌ها را قبل از اینکه اقدام به حمله کنند شناخته و از بین ببرند یا در بعضی موارد حداقل قدرت حمله‌ی آنها را به حداقل برسانند. در این سمینار؛ ابتدا به بررسی اجمالی باتنت‌ها و توپولوژی‌ها مختلف ارتباطی آنها پرداخته شده و روند تغییر و تکامل آنها را بررسی کرده‌ایم. سپس روش‌های مختلف تشخیص حمله را بررسی و آنها را براساس نحوه‌ی عملکردشان دسته‌بندی و مورد مطالعه قرار داده‌ایم و مزایا و معایب هر کدام را بیان کرده‌ایم. روش‌های تشخیص باتنت هنوز در مراحل ابتدایی و اولیه‌اش قرار دارد و این حوزه برای متخصصین امنیت جذاب است و جای بررسی بیشتر دارد.

کلمات کلیدی: حملات، باتنت، تشخیص باتنت، بدافزار

فصل اول

مقدمه

۱-۱- مقدمه

با پیشرفت پهنای‌باند شبکه‌ها و قدرت محاسبات ماشین‌ها، امروزه محاسبات توزیع شده به وفور مورد استفاده قرار می‌گیرد. در این راستا هکرها هم از این مفهوم برای انجام حملات قدرتمندتری استفاده می‌کنند [1]. روش‌هایی که امروزه برای بدست آوردن سود از باتنت‌ها وجود دارند عبارتنداز اجاری باتنت به شخصی دیگر برای ارسال نامه‌های ناخواسته، اخاذی از شرکت‌ها در مقابل حملات DDoS، سرقت اطلاعات شخصی افراد مثل اطلات کارت‌های اعتباری آن‌ها و غیره[2]. بر اساس مطالعات اخیر، حدود ۱۰ درصد از تمامی کامپیوترهای موجود بر روی اینترنت توسط باتنت‌ها آلوده شده‌اند. واژه بات از روبات برگرفته شده و در حقیقت یک کد دودویی بدخواه است که بر روی میزبان‌های آسیب‌پذیر اجرا شده و به مهاجم (که با نام مدیر بات شناخته می شود) امکان می‌دهد تا از راه دور آن میزبان‌ها را با فرامین خود هدایت نماید. باتنت نیز به معنی شبکه‌ای از میزبان‌های آلوده به بات می‌باشد. برخی اوقات به یک سیستم آلوده به بات، زامبی و به یک با تنت، ارتش زامبی گفته می‌شود. زمانی که یک کامپیوتر به بات آلوده می‌شود، دیگر قادر نخواهد بود در برابر دستورات مدیر بات مقاومت کرده یا از اجرای آنها سر باز زند. در نتیجه مهاجم می‌تواند از توان پردازشی میزبان‌های به تصرف در آمده، به صورت توزیع شده، به نفع خود بهره‌برداری کرده و انواع مختلفی از حملات را به صورت هماهنگ و با قدرت تخریبی بسیار بالا بر روی قربانی سازماندهی کند. این در حالی است که معمولاً هویت وی مخفی می‌ماند. اندازه یک بات نت به پیچیدگی و تعداد کامپیوترهای تصرف شده در این بات نت بستگی دارد. به دلیل اینکه باتنت‌ها از تکنولوژی‌های بدافزاری مختلفی تشکیل شده‌اند، توضیح دادن درباره آن‌ها و پیچیدگی کار آن‌ها چندان ساده نیست. مهاجمین تکنولوژی‌های مختلفی را به نحوی با هم ترکیب می‌کنند که دسته‌بندی آن‌ها را سخت می‌کند. باتنت‌ها برای مجرمان اینترنتی جذاب هستند، چون این قابلیت را دارند که برای جرایم

مختلف تنظیم مجدد گردند، برای سرویس‌های میزبانی جدید تغییر مکان پیدا کنند و در پاسخ به پیشرف تهای جدید امنیتی دوباره برنامه‌ریزی گردند. برخلاف دیگر بدافزارها که به طور مستقل از هم کار می‌کنند، یک باتنت به یک زیرساخت ارتباطی نیاز دارد تا مدیر بات بتواند از طریق آن، فرامین خود را برای بات‌ها ارسال کرده و پاسخ آن‌ها را دریافت کند. این زیرساخت ارتباطی با نام کانال فرمان و کنترل شناخته می‌شود. در واقع باتنت، یک گروه هماهنگ از بات‌هایی است که از طریق کانال فرمان و کنترل هدایت شده و فعالیت‌های بدخواهانه‌ای را انجام می‌دهند. در سال‌های اخیر، روش‌های مختلفی برای تشخیص باتنت‌ها پیشنهاد شده است[3][4][5]. اما بیشتر آن‌ها دارای محدودیت‌هایی هستند. اکثر این روش‌ها برای تشخیص باتنت‌ها به ساختار و یا پروتکل خاصی از کانال فرمان و کنترل یک باتنت وابسته هستند، در نتیجه قادر به تشخیص همه انواع باتنت‌ها نمی‌باشند. همچنین، اغلب آن‌ها توانایی تشخیص باتنت‌ها را در مراحل آغازین از چرخه حیات یک باتنت ندارند. بنابراین، نمی‌توانند باتنت‌ها را قبل از انجام فعالیت‌های بدخواهانه تشخیص دهند. در سوی دیگر، برخی از روش‌های ارائه شده به صورت غیر برخط عمل می‌کنند که این مساله برای یک سیستم تشخیص بدافزار یک ضعف عمده به شمار می‌آید. تشخیص باتنت‌ها مستقل از ساختار و پروتکل فرمان و کنترل آن‌ها می‌بایست بدون دانش قبلی از نمونه دودویی بات‌ها، نحو کانال‌های فرمان وکنترل و در نتیجه امضای باتنت صورت گیرد. بنابراین، برای ارائه روشی مقاوم نسبت به تغییرات و تکامل کانال‌های فرمان، باید ویژگی‌های ذاتی ارتباطات و فعالیت‌های باتنت مورد مطالعه قرار گیرد. در ادامه این سمینار ابتدا در بخش دوم به بررسی ویژگی باتنت‌ها و موضوعات مربوط به آنها پرداخته می‌شود. سپس در فصل سوم روش‌ها تشخیص باتنت‌ها دسته‌بندی و بررسی می‌گردد و همچنین سعی می‌شود مشکلات اصلی روش مذکور مطرح و جهت بهبود آن راه‌حل‌هایی پیشنهاد شود. در فصل چهارم هم نتیجه‌گیری و پیشنهادات بیان می‌شود.