عنوان مقاله:
کشف و تحلیل حملات Botnetدر شبکه های گسترده

محل انتشار:
دومین همایش ملی مهندسی رایانه و مدیریت فناوری اطلاعات (سال: 1394)

تعداد صفحات اصل مقاله: 9

نویسندگان:
طیبه شوکت پور - *کارشناسی ارشد نرم افزار، کامپیوتر، دانشگاه آزاد اسلامی واحد تهران مرکزی.*

رضا روانمهر - *عضو هیات علمی دانشگاه آزاد اسلامی واحد تهران مرکزی.*

خلاصه مقاله:
امروزه برای بخش قابل توجهی از حملاتی که در مقیاس اینترنت صورت میگیرد، از باتنتها استفاده میشود. باتنت، شبکهای از سیستمهای آلودهی متصل به اینترنت است که تحت کنترل مهاجم قرار دارد. این نسل مدرن از بدافزارها، به عنوانابزاری مناسب مورد توجه خرابکاران اینترنتی قرار دارد. مهاجمین، پس از تصرف سیستمهای آسیب پذیر قربانیان، میتوانند با استفاده از آنها، حملات اینترنتی مختلفی از قبیل ارسال هرزنامه، حملات جلوگیری از سرویس توزیع شده، سرقت هویت و سایر فعالیتهای مجرمانه را در مقیاس بسیار بزرگ اجرا نمایند، در حالی که هویت اصلی فرد مهاجم مخفی باقی میماند. از این رو، تحقیقات گستردهای در زمینهی شناسایی و جلوگیری از آنها انجام شده است. در این نگارش، ضمن معرفی اجمالی باتنت و انواع آن، چند روش شناسایی باتنتها مورد بررسی و مقایسه قرار میگیرد و در انتها به نسل جدیدی از آنها پرداخته میشود

کلمات کلیدی:
حملات امنیتی، بدافزار، باتنت، باتنت مبتنی بر وب، تشخیص باتنت

لینک ثابت مقاله در پایگاه سیویلیکا: