15th International Conference on
Information Technology, Computer & Telecommunication

بررسی بات نت‌ها و تکنیک‌های شناخت آن

بهزاد سارانی

چکیده

در میان انواع متعدی از نرم افزارهای مخرب ، بات نت ها گسترده ترین و جدی ترین تهدیدی است که امروزه به طور معمول در حملات سایبری رخ می دهد.بات نت ها مجموعه از رایانه های در خطر هستند که از راه دور به وسیله bot master تحت زیرساخت مشترک C&C کنترل می شوند. گسترده بودن حوزه عملکرد، امکان پنهان بودن عامل انسانی، بات نت ها را به موضوع مورد علاقه خرابکاران حوزه فناوری اطلاعات تبدیل کرده است.

از طرف دیگر تنوع زیاد در ساختارها و قراردادهای استفاده شده در بات نت ها، شناسایی آنها را بسیار دشوار نموده است. تحقیقهای بسیاری تاکنون در زمینه شناخت این شبکه ها انجام شده که هر کدام به شناسایی نو خاصی از بات نت پرداخته است. بات نت چیزی جز یک ابزار نیست و انگیزه های مختلفی برای استفاده از آنها وجود دارد. رایج ترین استفاده از بات نت انگیزه های مانند کسب درامد و برای اهداف خرابکارانه است .

در سال های اخیر، روش های متفاوتی برای تشخیص کانال های فرمان و کنترل بات نت ها پیشنهاد شده است. از این رو، مدیران بات سعی می کنند کانال های فرمان و کنترل جدیدی برای فرار از روشهای تشخیص موجود توسعه دهند. به همین دلیل کانال های فرمان و کنترل نسل های آینده بات نت ها درحال تحول به سمت ارتباطات پنهان و پیچیده است. استفاده از کانال های پنهان زمانی در بات نت های نسل های آینده این پیچیدگی را افزایش داده وکانال ها را مخفی تر می کند، چرا که تشخیص ترافیک آلوده ازترافیک سالم مشکل است.

واژگان کلیدی: بات نت، C&C،کانال فرمان وکنترل، هانی نت، بات مستر