

## عنوان مقاله:

بررسی روشهای تشخیص Botnet ها

## محل انتشار:

سومین همایش ملی مهندسی برق کامپیوتر و فناوری اطلاعات (سال: ۱۳۸۹)

تعداد صفحات اصل مقاله: ۷

## نویسندگان:

محسن رضوانی - دانشکده کامپیوتر و فناوری اطلاعات دانشگاه صنعتی شاهرود

ابوالفضل سرکرده پی - دانشجوی کارشناسی ارشد هوش مصنوعی دانشگاه صنعتی شاهرود

## خلاصه مقاله:

امروزه استفاده از Botnet ها به عنوان ابزاری جهت انجام فعالیتهای مجرمانه ای با وسعت زیاد در شبکه های کامپیوتری علیه اهداف وسیع مانند یک کشور بسیار افزایش یافته است Botnet محیط توزیع شده ای است که از آن جهت حملات مختلف با حجم وسیع استفاده می شود از این جهت امروزه تشخیص این نوع حملات به عنوان یکی از مسائل مهم در امنیت شبکه های کامپیوتری مطرح شده است در این مقاله پس از بررسی روشهای مطرح شده در این زمینه روشی که با بررسی ترافیک DNS ترافیک ایجاد شده توسط BOT ها را از ترافیک قانونی ایجاد شده بر روی یک سرور DNS با تعریف فعالیتهای گروهی تشخیص می دهد انتخاب شده و با تحلیل آن مشکلات آن بدست آمده و در جهت رفع آن پیشنهاداتی مطرح شده است

## کلمات کلیدی:

شبکه بات ها، Botnet، DNS-Based، Bot

## لینک ثابت مقاله در پایگاه سیویلیکا:

<https://civilica.com/doc/۱۰۶۱۹۷>