نوزدهمین کنفرانس ملی سالانه انجمن کامپیوتر ایران
دانشکده مهندسی کامپیوتر، دانشگاه شهید بهشتی، تهران، ۱۵-۱۳ اسفندماه ۱۳۹۲

یوتاب: روشی جدید مبتنی بر تحلیل‌های شباهت و شکست جریان‌های شبکه برای تشخیص بات‌نت‌های نسل جدید

رحیمه خدادادی [۱]، مهدی آبادی [۲]، بهزاد اکبری [۳]

[۱] گروه مهندسی کامپیوتر، واحد علوم و تحقیقات، دانشگاه آزاد اسلامی، قزوین
r.khodadadi@qiau.ac.ir

[۲] استادیار، گروه مهندسی کامپیوتر، دانشکده مهندسی برق و کامپیوتر، دانشگاه تربیت مدرس، تهران
abadi@modares.ac.ir

[۳] استادیار، گروه مهندسی کامپیوتر، دانشکده مهندسی برق و کامپیوتر، دانشگاه تربیت مدرس، تهران
b.akbari@modares.ac.ir

چکیده

یکی از ویژگی‌های ذاتی هر بات‌نت انجام فعالیت‌های گروهی توسط میزبان‌های آلوده به بات است. این میزبان‌ها فرامین یکسانی را دریافت کرده و فعالیت‌های مخرب مشابهی را انجام می‌دهند که باعث می‌شود جریان‌های شبکه آن‌ها شباهت زیادی با هم داشته باشند. علاوه بر آن، جریان‌های شبکه هر میزبان آلوده به بات ممکن است به دلایل مختلفی از قبیل خرابی سرویس‌دهندگان فرمان و کنترل، وجود دیواره‌های آتش فعال، تولید نام‌های دامنه الگوریتمی و غیره با شکست مواجه شوند. در سال‌های اخیر روش‌های زیادی برای تشخیص بات‌نت‌ها مبتنی بر تحلیل شباهت یا تحلیل شکست جریان‌های شبکه پیشنهاد شده است. در این مقاله، روشی جدید با نام یوتاب پیشنهاد می‌شود که از ترکیب هر دو تحلیل فوق برای تشخیص بات‌نت‌های نسل جدید استفاده می‌کند. در این روش، ترافیک شبکه به عنوان ورودی دریافت شده و برای هر یک از جریان‌های TCP، UDP و DNS یک بردار ویژگی استخراج می‌شود. سپس با خوشه‌بندی این بردارهای ویژگی، میزبان‌های دارای فعالیت‌های گروهی مشکوک و با محاسبه نرخ شکست جریان، میزبان‌های دارای شکست‌های مشکوک شناسایی می‌شوند. در نهایت، شهرت منفی میزبان‌ها مبتنی بر سابقه فعالیت‌های گروهی و سابقه شکست‌های مشکوک آن‌ها محاسبه شده و میزبان‌های دارای شهرت منفی بالا به عنوان میزبان‌های آلوده به بات گزارش می‌شوند. نتایج آزمایش‌های انجام شده برای تشخیص سه بات‌نت متفاوت نشان می‌دهند که روش پیشنهادی قادر است این بات‌نت‌ها را با نرخ هشدار نادرست پایین تشخیص دهد.

کلمات کلیدی

تشخیص بات‌نت، جریان شبکه، تحلیل شباهت، خوشه‌بندی، تحلیل شکست، نرخ شکست جریان، شهرت منفی.

۱- مقدمه

امروزه مهاجمین اینترنتی از بات‌نت‌ها[۱] برای انجام فعالیت‌های غیرقانونی از قبیل ارسال هرزنامه، حمله‌های جلوگیری از سرویس توزیعی، سرقت اطلاعات محرمانه و غیره سوءاستفاده می‌کنند. هر بات‌نت شامل گروهی از بات‌ها یا میزبان‌های آلوده به کد مخرب یکسان است که از راه دور و از طریق یک بستر ارتباطی با نام کانال فرمان و کنترل (C&C[۲]) هدایت می‌شوند. بات‌نت‌ها بر اساس ساختار کانال‌های فرمان و کنترل خود به دو دسته متمرکز و غیرمتمرکز تقسیم می‌شوند. در بات‌نت‌های متمرکز، مدیر بات یک میزبان با پهنای باند بالا را به عنوان نقطه مرکزی (سرویس‌دهنده فرمان و کنترل) انتخاب کرده و بر روی این میزبان سرویس‌های شبکه‌ای خاصی را برای