به نام خدا

جلسه ارائه هفتگی آزمایشگاه امنیت داده و شبکه

تشخیص شبکه‌های بات مبتنی بر ترافیک کارگزار نام دامنه

Botnet detection based on DNS traffic analysis

الهه سلطان آقایی

زمان: شنبه 2 دی ماه، ساعت 9 صبح

مکان: دانشکده‌ی مهندسی کامپیوتر، طبقه‌ی پنجم، DNSL

همواره مجرمان سایبری به دنبال کشف راه‌های جدید برای پوشش آثار فعالیت‌های مخرب خود و حفظ درآمد غیرقانونی هستند. یکی از ابزارهای جدید مورد استفاده، شبکه‌های بات است. یکی از ویژگی‌های اصلی شبکه-های بات دریافت دستورات اجرایی از کارگزار C&C است. در نتیجه، پنهان ماندن کارگزار C&C یکی از الزامات فعالیت این شبکه‌ها است. امروزه برای محافظت از این کارگزار از تکنیک‌های جدیدی مانند تغییرات پی‌درپی (fast-flux) استفاده می‌شود که خود شامل زیرگروه‌های single flux، double flux و domain flux است. از آنجایی که بات‌های متمرکز برای ارتباط با بات‌مستر خود نیاز به یافتن آدرس IP آن دارند، تحلیل ترافیک نام دامنه روشی کارآمد برای تشخیص این گروه از بات‌ها خواهد بود. در تحلیل ترافیک نام دامنه از دو رویکرد "فعال" و "غیرفعال" استفاده شده است. در رویکرد "فعال" پژوهشگر با اجرای پرس‌وجو بر روی کارگزار نام دامنه به کشف رابطه دامنه‌ها با یکدیگر می‌پردازد که این کار خود باعث ایجاد ترافیک می‌شود و می‌تواند بر روی رفتار بات تاثیرگذار باشد. در رویکرد "غیرفعال" نیز با تحلیل ترافیک موجود به صورت پنهانی رفتار بات بررسی می‌شود. در این ارائه، ضمن مروری بر انواع تکنیک‌های تغییر پی‌درپی، راه‌حل‌های پیشنهادی برای تشخیص هریک از این تکنیک‌ها ارائه خواهند شد و ضعف‌های هر یک از این روش‌ها بررسی و مقایسه می‌شوند.

شرکت در این جلسه برای تمامی دانشجویان علاقه‌مند آزاد است.