عنوان مقاله:
تهدید مانای پیشرفته؛ آشکارِ ناپیدا

محل انتشار:
هفدهمین کنفرانس بین المللی انجمن رمز ایران (سال: 1399)

تعداد صفحات اصل مقاله: 6

نویسنده:
امیر محمدزاده لاجوردی - *دکتری مهندسی کامپیوتر، دانشگاه صنعتی شریف، تهران*

خلاصه مقاله:
حملات سایبری پیشرفته ای که متوجه زیرساخت های حساس و حیاتی کشورهاست عموماً به عنوان تهدید مانای پیشرفته (Advanced Persistent Threat) شناخته می شود. از آنجا که در برخی از پژوهش ها و مستندات فنیِ منتشر شده، به اشتباه هر نوع حمله ای را تهدید مانای پیشرفته می نامند، در این سخن رانی تعریفی دقیق از این گونه حملات بر اساس کالبدشکافی نمونه های واقعی از تهدیدهای مانای پیشرفته ارائه می شود. شواهد نشان می دهد که این حملات دارای سه خاصیت اصلی آهستگی، سطح پایین، و ترکیبی بوده و همین خواص است که ابزارهای تشخیص نفوذ و همبسته سازیه شدار موجود را در شناسایی این گونه حملاتناتوان می سازد. در الگوی رفتار آهسته، بدافزار با استفاده از ترفندهایی، همانند توابع خواب و بیدار، فاصله بین گام های حمله را افزایش داده و رفتار خود را از دید سامانه های تشخیص، که دارای پنجره زمانی کوتاه مدت هستند، پنهان می سازد. در حملات مانای پیشرفته ی سطح پایین، مهاجم با استفاده از عامل ها و رفتارهای معتمد، و ترفندهایی همانند تزریق کد و یا سرقت گواهی نامه های دیجیتال، هرگونه ناهنجاری را پنهان کرده و به صورت ضمنی به نقض خط مشی های امنیتی می پردازد. از دیگر نقاط ضعف سامانه های موجود که در حملات مانای پیشرفته ترکیبی مورد سوء استفاده قرار می گیرد، عدم همبسته سازی رویدادهای سامانه ی عامل با رویدادهای شبکه، و استفاده از همبسته سازی هشدار به جای همبسته سازی رویداد است. در ادامه این سخن رانی و پس از بیان خلاء های موجود و ذکر دلایل ناکارآمدی ابزارهای تشخیص نفوذ و همبسته سازی هشدار، پیشنهادهایی برای حل این مشکلات و همچنین زمینه های پژوهشی موجود ارائه خواهد شد.

کلمات کلیدی:
تهدید مانای پیشرفته، بدافزار، تشخیص نفوذ، همبسته سازی هشدار، حمله آهسته، حمله سطح پایین، حمله ترکیبی.

لینک ثابت مقاله در پایگاه سیویلیکا: