عنوان طرح

پلتفرم تحلیل بدافزار بیت بان

مجری
شرکت بیت‌بان
(آزمایشگاه بیت‌بان)

نماینده
دکتر امیر محمدزاده لاجوردی

همکاران
امیر گوران اوریمی، مصطفی محمودیان دهکردی و رامتین باقری

چکیده‌ی طرح

طراحی و پیاده‌سازی یک پلتفرم تحلیل بدافزار که یک فایل را در سطوح مختلف از لحاظ ماهیت فایل (بد افزار یا سالم بودن) مورد ارزیابی و تحلیل قرار می‌دهد. بخش اصلی پلتفرم، هسته‌ی آن است که شامل پنج زیرسامانه ضد بد افزار مرکب(MultiAV)، تحلیل ایستا(Static Analysis)، تحلیل پویا(Dynamic Analysis)، تحلیل تخصصی دستی(Expert Analysis) و شناسایی منشاء انتشار بدافزار (Malware Origins) است.

در بخش ضد ویروس مرکب (MultiAV) یک فایل توسط ابزارهای ضد بد افزار مختلف مورد تحلیل و بررسی قرار می گیرد. یکی از مشکلات موجود در این بخش تحریم ایران توسط شرکت‌های تحلیل بد افزار و عدم ارائه‌ی API بود. برای رفع این مشکل با مهندسی معکوس ابزارهای ضد بد افزار این API از آن‌ها استخراج گردید. چنانچه یک فایل توسط ضد ویروس مرکب مخرب تشخیص داده نشد؛ فایل در بخش بعدی به صورت ایستا و پویا تحلیل می‌شود. در این بخش با طراحی و پیاده‌سازی یک جعبه شن (Sandbox) بر اساس فناوری Intel-VT، بدافزار در محیط ایزوله اجرا و رفتار آن مورد تحلیل قرار می گیرد. در فرآیند تحلیل فایل، ممکن است ضدویروس مرکب و جعبه شن قادر به شناسایی آن نباشند بنابراین نیازمند تحلیل توسط متخصصان انسانی هستیم. یکی از چالش‌های موجود در این فناوری نبود گروه تحلیل در شرکت‌ها و یا سربار مالی زیاد آنان در ایران است برای حل این مشکل در این پلتفرم تمام تحلیل گران بد افزار سراسر دنیا امکان ثبت نام، درج گزارش تحلیل فایل و دریافت مبلغ را دارند. به عبارت دیگر این پلتفرم بستری برای حضور و درآمدزایی تحلیلگران تهیه نموده است. در مرحله‌ی بعد منشاء انتشار بد افزار مشخص می گردد. در این بخش پروفایلی برای کانال‌های شبکه‌های اجتماعی همانند تلگرام و... تهیه و مشخص می‌شود؛ که منشاء انتشار بدافزار کجا بوده است.