

رتبه دوم پژوهش‌های کاربردی

گروه تخصصی برق و کامپیوتر

عنوان طرح

پلتفرم تحلیل بدافزار بیت بان

همکاران

امیر گوران اوریمی، مصطفی محمودیان دهکردی و رامتین باقری

مجری

شرکت بیت بان (آزمایشگاه بیت بان)

نماینده

دکتر امیر محمد زاده لاجوردی



چکیده‌ی طرح

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

در بخش ضد ویروس مرکب (MultiAV) یک فایل توسط ابزارهای ضد بدافزار مختلف مورد تحلیل و بررسی قرار می‌گیرد. یکی از مشکلات موجود در این بخش تحریم ایران توسط شرکت‌های تحلیل بدافزار و عدم ارائه‌ی API بود. برای رفع این مشکل با مهندسی معکوس ابزارهای ضد بدافزار 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 می‌گیرد. در فرآیند تحلیل فایل، ممکن است ضد ویروس 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 سربرار مالی زیاد آنان در ایران است برای حل این مشکل در این پلتفرم تمام تحلیل‌گران بدافزار 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 منشأ انتشار بدافزار مشخص می‌گردد. در این بخش پروفایلی برای کانال‌های شبکه‌های اجتماعی همانند تلگرام و... تهیه و مشخص می‌شود؛ که منشأ انتشار بدافزار کجا بوده است.



نام تهدیدافزار	سیستم عامل	نسخه	آخرین بروزرسانی	نتیجه
COMODO Internet Security	Windows	8.2.0.4703	۳۳ ساعت پیش	Win Worm GameThief.Nilage - CRSA@t3aanan
Immunet (ClamAV)	Windows	7.0.2.11454	۳۳ روز پیش	Win Worm.Viking.tpd
Dr.Web Security Space	Windows	11.0.5.96020	۳۳ ساعت پیش	Win.M.H.L.W.Game.F.v
ESET Smart Security	Windows	10.1.235.4	۳۳ ساعت پیش	Win.M.Viking.BR.virus
BitDefender	Windows	1.1	۳۳ ساعت پیش	TrojWare.Win.M.Viking.GameThief.Nilage
Kaspersky Total Security 17.0.0	Windows	17.0.0.853	۳۳ ساعت پیش	Worm.Win.M.Viking.bt
Webroot SecureAnywhere	Windows	9.0.26.61	۳۳ ساعت پیش	W.M.Malware.Hour
G DATA ANTI VIRUS	Windows	25.0.2.2	۲ روز پیش	Generic.Viking.Exx.A.DCCX
Microsoft Windows Defender	Windows	4.10.209.0	یک ماه پیش	Virus.Win.M.Viking.V