عنوان فارسی مقاله :

تشخیص کد خرابکار ناشناخته با استفاده از تکنیک های دسته بندی روی الگوهایOpCode

عنوان انگلیسی مقاله :

Detecting unknown malicious code by applying classification techniques on OpCode patterns

توجه !

این فایل تنها قسمتی از ترجمه میباشد. برای تهیه مقاله ترجمه شده کامل با فرمت ورد (قابل ویرایش) همراه با نسخه انگلیسی مقاله، اینجا کلیک نمایید.

6. Discussion and Conclusions

In this study we used OpCode *n*-gram patterns generated by disassembling the inspected executable files to extract features from the inspected files. OpCode *n*-grams are used as features during the classification process with the aim of identifying unknown malicious code. We performed an extensive evaluation using a test collection comprising more than 30,000 files. The evaluation consisted of three experiments.

6. بحث و نتیجه گیری

در این مطالعه از الگوهای OpCode n-gram تولید شده از طریق دیس اسمبل کردن فایلهای اجرایی مشکوک برای استخراج ویژگیها از فایل های مشکوک استفاده کردیم. از OpCode n-gram در طول فرایند دسته بندی به عنوان ویژگیهایی با هدف شناسایی کدهای خرابکار ناشناخته استفاده شده است.در این راستا یک ارزیابی گسترده با استفاده از مجموعه تست متشکل از بیش از 30000 فایل اجرا کردیم. ارزیابی از سه آزمایش تشکیل می شد.

توجه !

این فایل تنها قسمتی از ترجمه میباشد. برای تهیه مقاله ترجمه شده کامل با فرمت ورد (قابل ویرایش) همراه با نسخه انگلیسی مقاله، اینجا کلیک نمایید.

همچنین برای مشاهده سایر مقالات این رشته اینجا کلیک نمایید.