مجموعه وبینارهای
معاونت پژوهشی دانشکده مهندس کامپیوتر
هفته پژوهش گرامی باد

آقای دکتر محمد هادی علاییان
استادیار دانشکده مهندسی
کامپیوتر

On the Identification and Detection of Hidden Malware Behaviors

The malware analysis process is one of the most difficult, complex, tedious, and time-consuming steps of the malware detection process. Governments have supported and funded for identifying the malware automatically. Several automated techniques have been developed. Despite lots of supports and funds, the number of cyber-attacks is growing. Since signature-based malware detection techniques have non-solved problems to clarify polymorphism and metamorphism malware, researchers and antimalware companies have used malicious behavioral patterns. However, it does not solve the problem of the daily increase in the number of cyber-attacks. We clarified that identifying non-correct and non-accurate behavior is the main problem of behavioral analysis. Also, each behavior is the reflex of an event. Hidden behaviors observe when the conditions that trigger the behavior be provided. There is a question of what the requirements are. A behavior can be modeled by a graph that has vertexes and edges. Vertexes describe system calls, and edges illustrate the relation of system calls. Another problem is the merge of graphs in different conditions that malware is analyzed. The point is a set of truth behavior can throw a malicious behavior. A problem is the fusion of behaviors. Therefore, conducting a layered architecture of benign behavior that describes malicious behavior can be helpful. Consequently, a layered graph-based model for malware can be generated that involves environmental conditions. These conditions can be applied to the malware in an isolated or limited sandbox. Another problem is generating a non-detectable sandbox .

سه شنبه ۲۳ آذرماه ۱۴۰۰
ساعت ۱۷:۳۰ تا ۱۸

Link: https://meetbk.kntu.ac.ir/b/zar-iaf-581