

Table 3. The Slicing

ID	#FSlicing	#SSlicing	Average Time
S1	5	4	13s
S2	3	3	61s
S3	0	0	-

The efAPI list found by our approach is shown in **Table 4**. The #Q stands for the number of samples quitting at the API, and the #A stands for the number of samples invoked the API.

Table 4. The efAPIs used by malware samples in the experiment

API	#Q	#A	API	#Q	#A
IsDebuggerPresent()	2	7	CreateMutex()	1	1
CheckRemoteDebuggerPresent()	0	1	RegQuery()	2	1
GetComputerName()	0	1	CreateFile()	1	3
GetUserName()	1	2			

Reference

1. Egele, M., Scholte, T., Kirda, E., Kruegel, C.: A Survey on Automated Dynamic Malware Analysis Techniques and Tools. *J. ACM Computing Surveys*, 1--49 (2010)
2. Kang, M.G., Yin, H., Hanna, S., McCamant, S., Song, D.: Emulating Emulation-Resistant Malware. In: *VMSec*, pp. 11-23. Chicago, Illinois, USA (2009)
3. Balzarotti, D., Cova, M., Karlberger, C., Kruegel, C., Kirda, E., Vigna, G.: Efficient Detection of Split Personalities in Malware. In: *Proceedings of the 17th Annual Network and Distributed System Security Symposium (NDSS'10)*. San Diego, USA (2010)
4. Xie, P.D., Lu, X.C., Su, J.S., Wang, Y.J., Li, M.J.: iPanda: A Comprehensive Malware Analysis Tool. In: *27th International Conference on Information Networking (ICOIN'13)*. Bangkok, Thailand (2013)
5. Lindorfer, M., Kolbitsch, C., Comparetti, P.M.: Detecting Environment-Sensitive Malware. In: *Proceedings of the 14th International Symposium on Recent Advances in Intrusion Detection (RAID'11)*, 2011, pp. 338--357. Menlo Park, California, USA (2011)
6. Agrawal, H., Horgan, J.R.: Dynamic Program Slicing. In: *Proceedings of the ACM SIGPLAN'90 Conference on Programming Language Design and Implementation*, pp. 246-256. (1990)