Detecting and Classifying Morphed Malwares: A Survey

Abstract

In this era, most of the antivirus companies are facing immense difficulty in detecting morphed malwares as they conceal themselves from detection. Malwares use various techniques to camouflage themselves so as to increase their lifetime. These obscure methods cannot completely impede analysis, but it prolongs the process of analysis and detection. This paper presents a review on malware detection systems and the progress made in detecting advanced malwares which will serve as a reference to researchers interested in working on advance malware detection systems.
- Szor P., 2005 "The Art of Computer Virus Research and Defence," Addison-Wesley Professional
- Alazab M. and Venkatraman S., Watters P. and Malazab Mo., 2011 "Zero-day malware detection based on supervised learning algorithms of Api call signatures," Proceedings of the Ninth Australasian Data Mining Conference, Ballarat, Australia
- Moskovitch R., Elovici Y. and Rokach L., 2008 "Detection of unknown computer worms based on behavioural classification of the host," Computational Statistics & Data Analysis
Detecting and Classifying Morphed Malwares: A Survey

Regional Conference, New York, USA, pp. 28-28
- Kuriakose J. and Vinod P., 2014 "Towards the detection of Undetectable Metamorphic malware," SIN&apos;apos;14, Glasgow, Scotland UK
- Tsyganok K., Anikeev M., Tumoyan E. and Babenko L., 2012 "Classification of polymorphic and metamorphic malwares samples based on their behaviour," &quot; SIN

- Vinod P., Laxmi V., Jain H., Golecha Y. K. and Gaur M. S., 2010 "MEDUSA: Metamorphic malware dynamic analysis using signature from API," &quot; SIN
- Reeves S. D. and Zhang Q, 2005 "MetaAware: Identifying Metamorphic Malware," &quot; National Science Foundation (NSF)
- Lakhotia A. and Chouchane M. R., 2006 "Using Engine signatures to detect Metamorphic malware," &quot; WORM, USA
- Bonfante G., Kaczmarek M. and Marion J., 2009 "Architecture of a Morphological
Detecting and Classifying Morphed Malwares: A Survey

- Malware Detector, &quot;Computer Virology, pp. 263–270
- Kaczmarek M., Bonfante G. and Marion J., 2007 &quot;Control Flow Graphs as Malware Signatures,&quot;
- Kruegel C., Kirda E., Mutz D., Robertson W. and Vigna G., 2005 &quot;Polymorphic Worm Detection using Structural Information of Executables,&quot; In RAID, Springer, Verlag, pp. 207–226
- Lee H. and Jeong K., 2008 &quot;Code Graph for Malware Detection,&quot; In International conference on Information Networking, ICOIN, IEEE, pp. 1–5
- Elhadi A. A. E., Maarof M. A. and Osman A. H, 2012 &quot;Malware Detection Based on Hybrid Signature Behaviour Application Programming Interface Call Graph,&quot; American Journal of Applied Sciences 9
- Saffaf M. N., &quot;Malware Analysis Bachelors Thesis,&quot; Helsinki Metropolis University of Applied Sciences, May 27, 2009
- Gong T., Tan X. and Zhu M., 2009 &quot;Malware Detection via Classifying With Compression,&quot; The 1st International Conference on Information Science and Engineering, (ICISE)
- Leder F., Steinbock B., and Martini P., 2009 &quot;Classification and Detection of Metamorphic Malware Using Value Set Analysis,&quot; In MALWARE, pp. 39 – 46
- Bayoglu B. and Sogukpinar I., 2012 &quot;Graph Based Signature Classes for Detecting Polymorphic Worms via Content Analysis,&quot; Computer Network, ISSN 1389-1286, pp. 832–844
- Saini, Gandotra E., Bansal D. and Sofat S., 2014 &quot;Classification of PE files using static analysis,&quot; SIN&amp;apos;14, Glasgow, Scotland, UK, ACM
- Gandotra E., Bansal D. and Sofat S., 2014 &quot;Integrated Framework for Classification of Malwares,&quot; SIN&amp;apos;14, Glasgow, Scotland, UK, ACM

Index Terms

Computer Science
Networks
Keywords
Malware Evolution  Polymorphic  Oligomorphic  Metamorphic  Obfuscation
Decryptor and Encryptor