Introduction to the Special Issue on Challenges and Trends in Malware Analysis

Malicious software (malware) has become one of the main threats to Internet security, with a sustained growth in complexity and volume during the last three decades. Malware has experienced an impressive evolution since the 1980s, moving from simple worms, backdoors, and file-infection viruses to multi-stage campaigns, complex platforms that support a variety of modules, and sophisticated evasion mechanisms that make analysis increasingly difficult [2]. A key reason for this evolution is the fact that the malware industry long ago acquired the role of a commodity [1, 3] in the underground cybercrime economy [4]. This prompted malware developers to continuously improve their arsenal of techniques tailored to make quick money in different ways, from click fraud and spamming to cryptocurrency mining and bank credentials theft.

The increasing sophistication and impact of malware attacks has gone hand-in-hand with a growing interest from both industry and academia in defense and analysis techniques. Traditional signature-based malware detection techniques are easily bypassed by samples using obfuscation, software packing, or other similar techniques [5]. In addition, malware often incorporates capabilities to detect the execution environment and change its behavior when it runs on an analysis system. In this ever-changing world, there is a need for a broader spectrum of techniques to understand, detect, and respond in a timely manner to the diverse nature of malware.

This special issue welcomed submissions on these important challenges, including survey studies and works presenting novel research and experimentation results on malware science. We selected three papers that report novel methodologies and results in two key areas of malware detection and analysis: malware targeting smartphone platforms and analysis techniques using **dynamic binary instrumentation (DBI).** Each submission was reviewed by at least three reviewers and went through two rounds of reviews that helped the authors to address the identified issues.

In the article "Dynamic Detection of Mobile Malware using Smartphone Data and Machine Learning," the authors explore the problem of detecting mobile malware using features related to performance counts (e.g., CPU, battery, and memory usage). These features can be obtained without requiring privileged access, making the approach highly applicable to current platforms. The authors present several machine learning models that are tested with a dataset of known mobile Trojans and show promising results.

ACM Reference format:
Ricardo J. Rodríguez, Xabier Ugarte-Pedrero, and Juan Tapiador. 2022. Introduction to the Special Issue on Challenges and Trends in Malware Analysis. *Digit. Threat.: Res. Pract.* 3, 2, Article 8 (June 2022), 2 pages.
https://doi.org/10.1145/3536319

Authors' addresses: R. J. Rodríguez, Dpto. de Informática e Ingeniería de Sistemas, Universidad de Zaragoza, Ed. Ada Byron, Calle María de Luna 1, Zaragoza, Av. de la Vega, 15, 28108 Madrid Spain; email: rjrodriguez@unizar.es; X. Ugarte-Pedrero, Cisco Systems, USA; email: xabipedr@cisco.com; J. Tapiador, Dept. Informática, Universidad Carlos III de Madrid, Avda. Universidad 30, 28911 Leganés, Madrid, Spain; email: jestevez@inf.uc3m.es.

2576-5337/2022/06-ART8 $15.00
https://doi.org/10.1145/3536319

The article "Evaluating Dynamic Binary Instrumentation Systems for Conspicuous Features and Artifacts" surveys existing anti-analysis methods used by malware authors to evade DBI analysis systems. The authors present the results of an evaluation of popular DBI systems against such methods and make their data available to the community.

In the article "Evasion and Countermeasures Techniques to Detect Dynamic Binary Instrumentation Frameworks," the authors also examine anti-instrumentation techniques that abuse DBI frameworks, as well as existing countermeasures. The article presents a taxonomy for classifying existing DBI evasion techniques and countermeasures to avoid them and highlights challenges and interesting areas of future work on this topic.

As guest editors, we would like to thank all authors who submitted articles to this special issue, as well as all the reviewers for their valuable comments, suggestions, and commitment to submit reviews in a timely manner. We also thank DTRAP Co-Editors-in-Chief, Arun Lakhotia and Leigh Metcalf, and ACM for their support and giving us the opportunity to work on this special issue.

Ricardo J. Rodríguez
Dpto. de Informática e Ingeniería de Sistemas, Universidad de Zaragoza, Spain
Xabier Ugarte-Pedrero
Cisco Systems, USA
Juan Tapiador
Universidad Carlos III de Madrid, Spain

Guest Editors

REFERENCES

[1] Juan Caballero, Chris Grier, Christian Kreibich, and Vern Paxson. 2011. Measuring pay-per-install: The commoditization of malware distribution. In *Proceedings of the 20th USENIX Conference on Security (SEC'11)* (San Francisco, CA). USENIX Association, Berkeley, CA, 1–16.

[2] A. Calleja, J. Tapiador, and J. Caballero. 2019. The MalSource dataset: Quantifying complexity and code reuse in malware development. *IEEE Transactions on Information Forensics and Security* 14, 12 (Dec 2019), 3175–3190.

[3] Chris Grier, Lucas Ballard, Juan Caballero, Neha Chachra, Christian J. Dietrich, Kirill Levchenko, Panayiotis Mavrommatis, Damon McCoy, Antonio Nappa, Andreas Pitsillidis, Niels Provos, M. Zubair Rafique, Moheeb Abu Rajab, Christian Rossow, Kurt Thomas, Vern Paxson, Stefan Savage, and Geoffrey M. Voelker. 2012. Manufacturing compromise: The emergence of exploit-as-a-service. In *Proceedings of the 2012 ACM Conference on Computer and Communications Security (CCS'12)* (Raleigh, North Carolina). Association for Computing Machinery, New York, 821–832. https://doi.org/10.1145/2382196.2382283

[4] Kurt Thomas, Danny Yuxing Huang, David Y. Wang, Elie Bursztein, Chris Grier, Tom Holt, Christopher Kruegel, Damon McCoy, Stefan Savage, and Giovanni Vigna. 2015. Framing dependencies introduced by underground commoditization. In *Proceedings of the 14th Annual Workshop on the Economics of Information Security (WEIS'15),* (Delft, The Netherlands, 3 June 22-23, 2015).

[5] Xabier Ugarte-Pedrero, Mariano Graziano, and Davide Balzarotti. 2019. A close look at a daily dataset of malware samples. *ACM Trans. Priv. Secur.* 22, 1, Article 6 (Jan. 2019), 30 pages.