Introduction to the Special Issue on Memory-Based Malware and Other Unconventional Threats

MARCUS BOTACIN, Texas A&M University, USA
URIEL KOSAYEV, CYMDALL, Israel
RUIMIN SUN, Florida International University, USA

Security is a complex problem and there is no one-size-fits-all solution. Therefore, the different views provided by industry, academia, government, and multiple stakeholders are complementary and much appreciated. However, publicizing and systematizing this diffuse knowledge is challenging, such that the DTRAP's mission is to make it easier. In this special issue on Memory-based Malware and Other Unconventional Threats, we attempted to move forward on the systematization and dissemination of the knowledge on malware attacks and detection techniques. We focused on memory-resident and non-conventional malware to bring to the literature updated knowledge from the field, as malware techniques tend to appear in practice before they are described in the literature.

We received and accepted two papers. We thank the authors for sharing their knowledge with us. In "IronNetInjector: Weaponizing.NET Dynamic Language Runtime Engines", Anthony Rose, Scott Graham, and Jacob Krasnov cover memory injection attacks, which are each time more popular among malware samples, and potential defensive measures, that can help us to defeat this type of threat. Whereas focused on .Net binaries, the discussion presented by the authors extrapolates to general memory management. In "Keeping Up with the Emotets: Tracking a Multi-Infrastructure Botnet", Oleg Boyarchuk, Sebastiano Mariani, Stefano Ortolani, and Giovanni Vigna discuss the evolution of a botnet and how attackers use different strategies over time and space to defeat defenses, thus requiring defenses to move along. The two papers interconnect as memory injection techniques are often part of the botnet infection chain. We hope the reading of these papers might provide readers with insightful thoughts about how to protect users in practice.

We would like to thank Leigh Metcalf and Arun Lakhotia for trusting us to serve as guest editors in this special issue. We also thank the ACM staff for all the support with the management tasks. We extend our thanks to all those who helped to distribute the Call For Papers, including our colleagues and the anonymous people on social media. Last but not least, we would like to thank all the reviewers, without whom this special issue would not be possible. We thank: Andy Gill, Aokun Chen, Aleksandra "hasherazade", Cassius Puodzius, Daniele Cono D'Elia, Paulo de Geus, and Thomas Roccia.

CCS Concepts: • **Computer systems organization → Processors and memory architectures**; • **Security and privacy → Intrusion/anomaly detection and malware mitigation**; *Software and application security.*

Additional Key Words and Phrases: malware, memory injection, botnet

ACM Reference Format:
Marcus Botacin, Uriel Kosayev, and Ruimin Sun. 2023. Introduction to the Special Issue on Memory-Based Malware and Other Unconventional Threats. *Digit. Threat. Res. Pract.* 1, 1, Article 1 (January 2023), 1 page. https://doi.org/TBD

Authors' addresses: Marcus Botacin, botacin@tamu.edu, Texas A&M University, USA; Uriel Kosayev, uriel@cymdall.com, CYMDALL, Israel; Ruimin Sun, rsun@fiu.edu, Florida International University, USA.

2576-5337/2023/1-ART1
https://doi.org/TBD