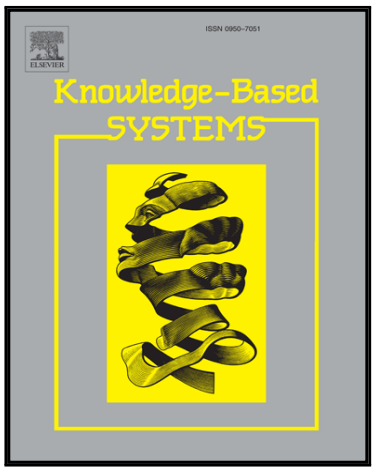

Trusted System-Calls Analysis Methodology Aimed at Detection of Compromised Virtual Machines Using Sequential Mining

Nir Nissim , Yuval Lapidot , Aviad Cohen , Yuval Elovici

PII: S0950-7051(18)30204-1
DOI: 10.1016/j.knosys.2018.04.033
Reference: KNOSYS 4315

To appear in: *Knowledge-Based Systems*

Received date: 10 January 2018
Revised date: 25 April 2018
Accepted date: 26 April 2018

Please cite this article as: Nir Nissim , Yuval Lapidot , Aviad Cohen , Yuval Elovici , Trusted System-Calls Analysis Methodology Aimed at Detection of Compromised Virtual Machines Using Sequential Mining, *Knowledge-Based Systems* (2018), doi: 10.1016/j.knosys.2018.04.033

Trusted System-Calls Analysis Methodology Aimed at Detection of Compromised Virtual Machines Using Sequential Mining

Nir Nissim[1,2], Yuval Lapidot[1,3] , Aviad Cohen[1,3] and Yuval Elovici[1,3]

[1]*Malware Lab, Cyber Security Research Center, Ben-Gurion University of the Negev, Beer-Sheva, Israel*

[2]*Department of Industrial Engineering and Management, Ben-Gurion University of the Negev, Beer-Sheva, Israel*

[3] *Department of Software and Information Systems Engineering, Ben-Gurion University of the Negev, Beer-Sheva, Israel*

Abstract

Most organizations today employ cloud-computing environments and virtualization technology; Due to their prevalence and importance in providing services to the entire organization, virtual-servers are constantly targeted by cyber-attacks, and specifically by malware. Existing solutions, consisting of the widely-used antivirus (AV) software, fail to detect newly created and unknown-malware; moreover, by the time the AV is updated, the organization has already been attacked. In this paper, we present a during run-time analysis methodology for a trusted detection of unknown malware on virtual machines (VMs). We conducted trusted analysis of volatile memory dumps taken from a VM and focused on analyzing their system-calls using a sequential-mining-method. We leveraged the most informative system-calls by machine-learning algorithms for the efficient detection of malware in widely used VMs within organizations (i.e. IIS and Email server). We evaluated our methodology in a comprehensive set of experiments over a collections of real-world, advanced, and notorious malware (both ransomware and RAT), and legitimate programs. The results show that our suggested methodology is able to detect the presence of unknown malware, in an average of 97.9% TPR and 0% FPR. Such results and capabilities can form the ground for the development of practical detection-tools for both corporates and companies.

Keywords: Sequential Mining, Volatile Memory, Memory Dump, Virtual Machine, Virtual Server, Private Cloud, Machine Learning, Malware Detection, Ransomware, Remote Access Trojan.