An I/O Request Packet (IRP) Driven Effective Ransomware Detection Scheme using Artificial Neural Network

Title	An I/O Request Packet (IRP) Driven Effective Ransomware Detection Scheme using Artificial Neural Network
Publication Type	Conference Paper
Year of Publication	2020
Authors	Ayub, M. A., Continella, A., Siraj, A.
Conference Name	2020 IEEE 21st International Conference on Information Reuse and Integration for Data Science (IRI)
Date Published	aug
Keywords	artificial neural network, compositionality, cryptography, cyber-attacks, Data collection, discovering novel ransomware families, driven effective ransomware detection scheme, effective artificial neural network structure, global surge, I/O Monitoring, industry-based security researchers, Information Reuse and Security, invasive software, IRP logs, Kernel, learning (artificial intelligence), low-level file system, Malware, Microsoft Windows, neural nets, Neural networks, newly found research paradigm, pubcrawl, ransomware, ransomware attacks, ransomware behavior, ransomware detection, ransomware families, ransomware researchers, ransomware samples, ransomware samples every day, Resiliency, retail to critical infrastructure

Abstract

In recent times, there has been a global surge of ransomware attacks targeted at industries of various types and sizes from retail to critical infrastructure. Ransomware researchers are constantly coming across new kinds of ransomware samples every day and discovering novel ransomware families out in the wild. To mitigate this ever-growing menace, academia and industry-based security researchers have been utilizing unique ways to defend against this type of cyber-attacks. I/O Request Packet (IRP), a low-level file system I/O log, is a newly found research paradigm for defense against ransomware that is being explored frequently. As such in this study, to learn granular level, actionable insights of ransomware behavior, we analyze the IRP logs of 272 ransomware samples belonging to 18 different ransomware families captured during individual execution. We further our analysis by building an effective Artificial Neural Network (ANN) structure for successful ransomware detection by learning the underlying patterns of the IRP logs. We evaluate the ANN model with three different experimental settings to prove the effectiveness of our approach. The model demonstrates outstanding performance in terms of accuracy, precision score, recall score, and F1 score, i.e., in the range of 99.7%±0.2%.

DOI 10.1109/IRI49571.2020.00053

Citation Key ayub_io_2020

malware Kernel invasive software learning (artificial intelligence) Resiliency pubcrawl Ransomware Cryptography neural nets Neural networks cyber-attacks Data collection microsoft windows Compositionality ransomware attacks ransomware detection artificial neural network ransomware families ransomware samples Information Reuse and Security discovering novel ransomware families driven effective ransomware detection scheme effective artificial neural network structure global surge I/O Monitoring industry-based security researchers IRP logs low-level file system newly found research paradigm ransomware behavior ransomware researchers ransomware samples every day retail to critical infrastructure