Trusted detection of ransomware in a private cloud usi leveraging meta-features from volatile memory

Expert Systems With Applications

102, 158-178

DOI: 10.1016/j.eswa.2018.02.039

Citation Report

#	Article	IF	Citations
1	A Framework for Analyzing Ransomware using Machine Learning. , 2018, , .		48
2	Malware Detection Based on Dynamic Multi-Feature Using Ensemble Learning at Hypervisor. , 2018, , .		3
3	A Survey on Security of Cloud Environment: Threats, Solutions, and Innovation. , 2018, , .		4
4	Novel set of general descriptive features for enhanced detection of malicious emails using machine learning methods. Expert Systems With Applications, 2018, 110, 143-169.	4.4	27
5	Volatile memory analysis using the MinHash method for efficient and secured detection of malware in private cloud. Computers and Security, 2019, 87, 101590.	4.0	21
6	TrustSign: Trusted Malware Signature Generation in Private Clouds Using Deep Feature Transfer Learning. , 2019, , .		15
7	Sec-Lib: Protecting Scholarly Digital Libraries From Infected Papers Using Active Machine Learning Framework. IEEE Access, 2019, 7, 110050-110073.	2.6	11
8	Dynamic Malware Analysis in the Modern Eraâ€"A State of the Art Survey. ACM Computing Surveys, 2020, 52, 1-48.	16.1	146
9	Keep an eye on your personal belongings! The security of personal medical devices and their ecosystems. Journal of Biomedical Informatics, 2019, 95, 103233.	2.5	22
10	Crypto-ransomware early detection model using novel incremental bagging with enhanced semi-random subspace selection. Future Generation Computer Systems, 2019, 101, 476-491.	4.9	61
11	A Survey on Situational Awareness of Ransomware Attacksâ€"Detection and Prevention Parameters. Remote Sensing, 2019, 11, 1168.	1.8	33
12	Malboard: A novel user keystroke impersonation attack and trusted detection framework based on side-channel analysis. Computers and Security, 2019, 85, 240-269.	4.0	18
13	Systematic literature review and metadata analysis of ransomware attacks and detection mechanisms. Journal of Reliable Intelligent Environments, 2019, 5, 67-89.	3.8	38
14	Intelligent and Dynamic Ransomware Spread Detection and Mitigation in Integrated Clinical Environments. Sensors, 2019, 19, 1114.	2.1	55
15	Ransomware Prediction Using Supervised Learning Algorithms. , 2019, , .		19
16	Endpoint Detection and Response: Why Use Machine Learning?. , 2019, , .		4
17	Malware Detection Based on Multi-level and Dynamic Multi-feature Using Ensemble Learning at Hypervisor. Mobile Networks and Applications, 2020, , 1.	2.2	12
18	A Pseudo Feedback-Based Annotated TF-IDF Technique for Dynamic Crypto-Ransomware Pre-Encryption Boundary Delineation and Features Extraction. IEEE Access, 2020, 8, 140586-140598.	2.6	38

#	Article	IF	Citations
19	Ensuring Anomaly-Aware Security Model for Dynamic Cloud Environment using Transfer Learning. , 2020, , .		0
20	Mind your privacy: Privacy leakage through BCI applications using machine learning methods. Knowledge-Based Systems, 2020, 198, 105932.	4.0	20
21	A proposed Crypto-Ransomware Early Detection(CRED) Model using an Integrated Deep Learning and Vector Space Model Approach. , 2020, , .		12
22	CardiWall: A Trusted Firewall for the Detection of Malicious Clinical Programming of Cardiac Implantable Electronic Devices. IEEE Access, 2020, 8, 48123-48140.	2.6	15
23	Early detection of crypto-ransomware using pre-encryption detection algorithm. Journal of King Saud University - Computer and Information Sciences, 2022, 34, 1984-1999.	2.7	17
24	Deep feature transfer learning for trusted and automated malware signature generation in private cloud environments. Neural Networks, 2020, 124, 243-257.	3.3	36
25	MalJPEG: Machine Learning Based Solution for the Detection of Malicious JPEG Images. IEEE Access, 2020, 8, 19997-20011.	2.6	23
26	Stretchable and Wearable Resistive Switching Randomâ€Access Memory. Advanced Intelligent Systems, 2020, 2, 2000007.	3.3	24
27	Internet of things and ransomware: Evolution, mitigation and prevention. Egyptian Informatics Journal, 2021, 22, 105-117.	4.4	99
28	Redundancy Coefficient Gradual Up-weighting-based Mutual Information Feature Selection technique for Crypto-ransomware early detection. Future Generation Computer Systems, 2021, 115, 641-658.	4.9	29
29	Detecting ransomware attacks using intelligent algorithms: recent development and next direction from deep learning and big data perspectives. Journal of Ambient Intelligence and Humanized Computing, 2021, 12, 8699-8717.	3.3	27
30	Novel Meta-Features for Automated Machine Learning Model Selection in Anomaly Detection. IEEE Access, 2021, 9, 89675-89687.	2.6	10
31	Ensemble-Based Stegomalware Detection System for Hidden Ransomware Attack. Lecture Notes in Networks and Systems, 2021, , 599-619.	0.5	3
32	Application of Machine Learning for Ransomware Detection in IoT Devices. Studies in Computational Intelligence, 2021, , 393-420.	0.7	12
33	Hypervisor-assisted dynamic malware analysis. Cybersecurity, 2021, 4, .	3.1	5
34	Automatic Learning Path Recommendation for Open Source Projects Using Deep Learning on Knowledge Graphs. , 2021, , .		3
35	Pay Attention: Improving Classification of PE Malware Using Attention Mechanisms Based on System Call Analysis. , 2021, , .		5
36	Leveraging malicious behavior traces from volatile memory using machine learning methods for trusted unknown malware detection in Linux cloud environments. Knowledge-Based Systems, 2021, 226, 107095.	4.0	29

#	Article	IF	Citations
37	Ransomware: Recent advances, analysis, challenges and future research directions. Computers and Security, 2021, 111, 102490.	4.0	64
38	TKRD: Trusted kernel rootkit detection for cybersecurity of VMs based on machine learning and memory forensic analysis. Mathematical Biosciences and Engineering, 2019, 16, 2650-2667.	1.0	20
39	Process based volatile memory forensics for ransomware detection. Concurrency Computation Practice and Experience, 0, , e6672.	1.4	6
40	Deep-Hook: A trusted deep learning-based framework for unknown malware detection and classification in Linux cloud environments. Neural Networks, 2021, 144, 648-685.	3.3	15
41	Clustering Analysis for Malware Behavior Detection using Registry Data. International Journal of Advanced Computer Science and Applications, 2019, 10, .	0.5	5
42	Buy/Hold/Trade or Sell/Divest/Disengage. Advances in Social Networking and Online Communities Book Series, 2019, , 121-202.	0.3	0
43	Developing a secured image file management system using modified AES. Bulletin of Electrical Engineering and Informatics, 2019, 8, .	0.6	3
45	Ransomware Mitigation in the Modern Era: A Comprehensive Review, Research Challenges, and Future Directions. ACM Computing Surveys, 2022, 54, 1-36.	16.1	32
46	Prognosis Negative: Evaluating Real-Time Behavioral Ransomware Detectors. , 2021, , .		3
47	Machine Learning and Feature Selection Based Ransomware Detection Using Hexacodes. Advances in Intelligent Systems and Computing, 2021, , 583-597.	0.5	3
48	An improved forensic-by-design framework for cloud computing with systems engineering standard compliance. Forensic Science International: Digital Investigation, 2022, 40, 301315.	1.2	3
49	Research on Educational Informatization Platform Based on Cloud Computing. Lecture Notes in Electrical Engineering, 2022, , 1140-1153.	0.3	2
50	A study on malicious software behaviour analysis and detection techniques: Taxonomy, current trends and challenges. Future Generation Computer Systems, 2022, 130, 1-18.	4.9	23
51	A Weighted Minimum Redundancy Maximum Relevance Technique for Ransomware Early Detection in Industrial IoT. Sustainability, 2022, 14, 1231.	1.6	20
52	A Chronological Evolution Model for Crypto-Ransomware Detection Based on Encrypted File-Sharing Traffic. SSRN Electronic Journal, 0, , .	0.4	0
53	Cloud-based data pipeline orchestration platform for COVID-19 evidence-based analytics. , 2022, , 159-180.		2
54	A Survey on Ransomware: Evolution, Taxonomy, and Defense Solutions. ACM Computing Surveys, 2022, 54, 1-37.	16.1	67
55	Pre-Encryption and Identification (PEI): An Anti-crypto Ransomware Technique. IETE Journal of Research, 2023, 69, 8058-8066.	1.8	2

#	Article	IF	Citations
56	A Survey of Crypto Ransomware Attack Detection Methodologies: An Evolving Outlook. Sensors, 2022, 22, 1837.	2.1	29
57	An effective ransomware detection approach in a cloud environment using volatile memory features. Journal of Computer Virology and Hacking Techniques, 2022, 18, 407-424.	1.6	5
58	Automated Dynamic Detection of Ransomware using Augmented Bootstrapping. , 2022, , .		2
59	File Packing from the Malware Perspective: Techniques, Analysis Approaches, and Directions for Enhancements. ACM Computing Surveys, 2023, 55, 1-45.	16.1	11
60	Crow Search with Adaptive Awareness Probability-Based Deep Belief Network for Detecting Ransomware. International Journal of Pattern Recognition and Artificial Intelligence, 2022, 36, .	0.7	1
61	Cloud-BlackBox: Toward practical recording and tracking of VM swarms for multifaceted cloud inspection. Future Generation Computer Systems, 2022, 137, 219-233.	4.9	1
62	Crypto-ransomware detection using machine learning models in file-sharing network scenarios with encrypted traffic. Expert Systems With Applications, 2022, 209, 118299.	4.4	9
63	Comprehensive review on intelligent security defences in cloud: Taxonomy, security issues, ML/DL techniques, challenges and future trends. Journal of King Saud University - Computer and Information Sciences, 2022, 34, 9102-9131.	2.7	7
64	An intelligent protection framework for intrusion detection in cloud environment based on covariance matrix self-adaptation evolution strategy and multi-criteria decision-making. Journal of Intelligent and Fuzzy Systems, 2023, , 1-31.	0.8	0
65	A Machine Learning Approach to Analyze Cloud Computing Attacks. , 2022, , .		0
66	A Review of the Various Machine Learning Algorithms for Cloud Computing. , 2022, , .		0
67	Learning-Based Artificial Algae Algorithm with Optimal Machine Learning Enabled Malware Detection. Computer Systems Science and Engineering, 2023, 46, 3103-3119.	1.9	0
68	The Age of Ransomware: A Survey on the Evolution, Taxonomy, and Research Directions. IEEE Access, 2023, 11, 40698-40723.	2.6	9
70	A Novel Malware Classification Method Based on Memory Image Representation. , 2023, , .		0
74	Ransomware-as-a-Weapon (RaaW). Advances in Information Security, Privacy, and Ethics Book Series, 2023, , 247-266.	0.4	0
75	A Recent Systematic Review of Ransomware Attack detection in machine learning techniques. , 2023, , .		0
79	A Systematic Literature Review of Ransomware Detection Methods and Tools for Mitigating Potential Attacks. Communications in Computer and Information Science, 2024, , 80-95.	0.4	0