# A Survey on malware analysis and mitigation technique

Computer Science Review

32, 1-23

DOI: 10.1016/j.cosrev.2019.01.002

Citation Report

| # | Article | IF | Citations |
|---|---|---|---|
| 1 | Software-defined forensic framework for malware disaster management in Internet of Thing devices for extreme surveillance. Computer Communications, 2019, 147, 14-20. | 3.1 | 8 |
| 2 | A Consistently-Executing Graph-Based Approach for Malware Packer Identification. IEEE Access, 2019, 7, 51620-51629. | 2.6 | 10 |
| 3 | Instrumenting API Hooking for a Realtime Dynamic Analysis. , 2019, , . | | 1 |
| 4 | Classification of malicious process using highâ€level activity based dynamic analysis. Security and Privacy, 2019, 2, e86. | 1.9 | 1 |
| 5 | Identifying Malicious Software Using Deep Residual Long-Short Term Memory. IEEE Access, 2019, 7, 163128-163137. | 2.6 | 25 |
| 7 | Contextual Identification of Windows Malware through Semantic Interpretation of API Call Sequence. Applied Sciences (Switzerland), 2020, 10, 7673. | 1.3 | 14 |
| 8 | Analysis of Security Mechanisms to Mitigate Hacker Attacks to Improve e-Commerce Management in Ecuador. , 2020, , . | | 1 |
| 9 | Development of Reinforcement Learning and Pattern Matching (RLPM) Based Firewall for Secured Cloud Infrastructure. Wireless Personal Communications, 2020, 115, 993-1018. | 1.8 | 13 |
| 10 | A proposed Crypto-Ransomware Early Detection(CRED) Model using an Integrated Deep Learning and Vector Space Model Approach. , 2020, , . | | 12 |
| 11 | A Malware Variant Resistant To Traditional Analysis Techniques. , 2020, , . | | 4 |
| 12 | A survey on machine learning-based malware detection in executable files. Journal of Systems Architecture, 2021, 112, 101861. | 2.5 | 101 |
| 13 | Automated malware identification method using image descriptors and singular value decomposition. Multimedia Tools and Applications, 2021, 80, 10881-10900. | 2.6 | 9 |
| 14 | Malware Behavior Through Network Trace Analysis. Lecture Notes in Networks and Systems, 2021, , 3-18. | 0.5 | 2 |
| 15 | Tight Arms Race: Overview of Current Malware Threats and Trends in Their Detection. IEEE Access, 2021, 9, 5371-5396. | 2.6 | 59 |
| 16 | An Adaptive Behavioral-Based Incremental Batch Learning Malware Variants Detection Model Using Concept Drift Detection and Sequential Deep Learning. IEEE Access, 2021, 9, 97180-97196. | 2.6 | 33 |
| 17 | Comparative Performance Analysis of Anti-virus Software. Communications in Computer and Information Science, 2021, , 430-443. | 0.4 | 1 |
| 18 | Early Detection of In-Memory Malicious Activity Based on Run-Time Environmental Features. Lecture Notes in Computer Science, 2021, , 397-404. | 1.0 | 0 |
| 20 | Trends and Challenges in Network Covert Channels Countermeasures. Applied Sciences (Switzerland), 2021, 11, 1641. | 1.3 | 34 |

| # | Article | IF | Citations |
|---|---|---|---|
| 21 | Malicious Traffic classification Using Long Short-Term Memory (LSTM) Model. Wireless Personal Communications, 2021, 119, 2707-2724. | 1.8 | 13 |
| 22 | Comparative analysis of Android and iOS from security viewpoint. Computer Science Review, 2021, 40, 100372. | 10.2 | 34 |
| 23 | A survey and taxonomy of program analysis for IoT platforms. Ain Shams Engineering Journal, 2021, 12, 3725-3736. | 3.5 | 6 |
| 24 | Malicious application detection in android â€" A systematic literature review. Computer Science Review, 2021, 40, 100373. | 10.2 | 31 |
| 25 | Vulnerability retrospection of security solutions for software-defined Cyberâ€"Physical System against DDoS and IoT-DDoS attacks. Computer Science Review, 2021, 40, 100371. | 10.2 | 49 |
| 26 | A threat model method for ICS malware. , 2021, , . | | 10 |
| 27 | Boosting training for PDF malware classifier via active learning. International Journal of Intelligent Systems, 2022, 37, 2803-2821. | 3.3 | 17 |
| 28 | Security Analysis and Bypass User Authentication Bound to Device of Windows Hello in the Wild. Security and Communication Networks, 2021, 2021, 1-13. | 1.0 | 2 |
| 29 | A Flow-based Multi-agent Data Exfiltration Detection Architecture for Ultra-low Latency Networks. ACM Transactions on Internet Technology, 2021, 21, 1-30. | 3.0 | 6 |
| 30 | Comprehensive Analysis of IoT Malware Evasion Techniques. Engineering, Technology & Applied Science Research, 2021, 11, 7495-7500. | 0.8 | 6 |
| 31 | Identifying meaningful clusters in malware data. Expert Systems With Applications, 2021, 177, 114971. | 4.4 | 4 |
| 32 | The Risk of Botnets in Cyber Physical Systems. , 2020, , 81-106. | | 5 |
| 33 | Advanced metering infrastructures. , 2020, , . | | 5 |
| 34 | A Novel Method for Detecting Advanced Persistent Threat Attack Based on Belief Rule Base. Applied Sciences (Switzerland), 2021, 11, 9899. | 1.3 | 5 |
| 35 | An IoT Botnet Prediction Model Using Frequency based Dependency Graph. , 2019, , . | | 2 |
| 36 | Introduction to Malware Analysis. Studies in Computational Intelligence, 2022, , 129-141. | 0.7 | 4 |
| 37 | Beyond Labeling: Using Clustering to Build Network Behavioral Profiles of Malware Families. , 2021, , 381-409. | | 6 |
| 38 | A Malware Detection Framework Based on Forensic and Unsupervised Machine Learning Methodologies. , 2020, , . | | 1 |

| # | Article | IF | Citations |
|---|---|---|---|
| 39 | A Quest for Best: A Detailed Comparison Between Drakvuf-VMI-Based and Cuckoo Sandbox-Based Technique for Dynamic Malware Analysis. Advances in Intelligent Systems and Computing, 2021, , 275-290. | 0.5 | 7 |
| 40 | MANIAC: A Man-Machine Collaborative System for Classifying Malware Author Groups. , 2021, , . | | 1 |
| 41 | Investigating Malware Propagation and Behaviour Using System and Network Pixel-Based Visualisation. SN Computer Science, 2022, 3, 1. | 2.3 | 1 |
| 42 | A Recent Research on Malware Detection Using Machine Learning Algorithm: Current Challenges and Future Works. Lecture Notes in Computer Science, 2021, , 469-481. | 1.0 | 5 |
| 43 | 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 |
| 44 | USING TRANSFER LEARNING FOR MALWARE CLASSIFICATION. International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences - ISPRS Archives, 0, XLIV-4/W3-2020, 343-349. | 0.2 | 6 |
| 45 | Security Threat and Vulnerability Assessment and Measurement in Secure Software Development. Computers, Materials and Continua, 2022, 71, 5039-5059. | 1.5 | 11 |
| 46 | Polymorphic Malware Behavior Through Network Trace Analysis. , 2022, , . | | 2 |
| 47 | On the Effectiveness of Image Processing Based Malware Detection Techniques. Cybernetics and Systems, 2022, 53, 615-640. | 1.6 | 7 |
| 48 | Tools and Techniques for Collection and Analysis of Internet-of-Things malware: A systematic state-of-art review. Journal of King Saud University - Computer and Information Sciences, 2022, 34, 9867-9888. | 2.7 | 11 |
| 49 | A pilot comparative analysis of the Cuckoo and Drakvuf sandboxes: An end-user perspective. Military Technical Courier, 2022, 70, 372-392. | 0.3 | 1 |
| 50 | A game model design using test bed for Malware analysis training. Information and Computer Security, 2022, ahead-of-print, . | 1.5 | 0 |
| 51 | CamoDroid: An Android application analysis environment resilient against sandbox evasion. Journal of Systems Architecture, 2022, 125, 102452. | 2.5 | 3 |
| 52 | Deep Learning for Malware Classification Platform using Windows API Call Sequence. , 2021, , . | | 1 |
| 53 | EthClipper: A Clipboard Meddling Attack on Hardware Wallets with Address Verification Evasion. , 2021, , . | | 5 |
| 54 | The Reliability Assessment for Advanced Persistent Threat Defense based on Correlation Evidence Reasoning Rule. , 2021, , . | | 0 |
| 55 | Malware Detection Approaches using Machine Learning Techniques- Strategic Survey. , 2021, , . | | 1 |
| 56 | A Taxonomy for Threat Actorsâ€™ Delivery Techniques. Applied Sciences (Switzerland), 2022, 12, 3929. | 1.3 | 3 |

| # | Article | IF | Citations |
|---|---|---|---|
| 57 | Malware Detection Using LightGBM With a Custom Logistic Loss Function. IEEE Access, 2022, 10, 47792-47804. | 2.6 | 7 |
| 58 | ConcSpectre: Be Aware of Forthcoming Malware Hidden in Concurrent Programs. IEEE Transactions on Reliability, 2022, 71, 1174-1188. | 3.5 | 1 |
| 59 | Deep-Ensemble and Multifaceted Behavioral Malware Variant Detection Model. IEEE Access, 2022, 10, 42762-42777. | 2.6 | 7 |
| 60 | Application of the SAMA methodology to Ryuk malware. Journal of Computer Virology and Hacking Techniques, 2023, 19, 165-198. | 1.6 | 2 |
| 61 | Utility of Binary Cuckoo Search Approach for Microarray Data Analysis. Advances in Healthcare Information Systems and Administration Book Series, 2022, , 12-31. | 0.2 | 0 |
| 62 | ModX. , 2022, , . | | 12 |
| 63 | MaliCage: A packed malware family classification framework based on DNN and GAN. Journal of Information Security and Applications, 2022, 68, 103267. | 1.8 | 2 |
| 65 | Malware Detection Issues, Challenges, and Future Directions: A Survey. Applied Sciences (Switzerland), 2022, 12, 8482. | 1.3 | 48 |
| 66 | A comprehensive review on detection of cyber-attacks: Data sets, methods, challenges, and future research directions. Internet of Things (Netherlands), 2022, 20, 100615. | 4.9 | 17 |
| 67 | Static Analysis of Malware. SpringerBriefs in Computer Science, 2022, , . | 0.2 | 1 |
| 68 | Towards Optimizing Malware Detection: An Approach Based onÂGenerative Adversarial Networks andÂTransformers. Lecture Notes in Computer Science, 2022, , 598-610. | 1.0 | 1 |
| 69 | Principles of Code-Level Analysis. SpringerBriefs in Computer Science, 2022, , . | 0.2 | 0 |
| 70 | Cyber Weapons and Artificial Intelligence: Impact, Influence and the Challenges for Arms Control. , 2022, , 145-158. | | 1 |
| 71 | Cybersecurity Infrastructure adoption Model for Malware Mitigation in Small Medium Enterprises (SME). , 2022, , . | | 1 |
| 72 | PDF Malware Detection Based on Optimizable Decision Trees. Electronics (Switzerland), 2022, 11, 3142. | 1.8 | 11 |
| 73 | Machine Learning and Hyperparameters Algorithms for Identifying Groundwater Aflaj Potential Mapping in Semi-Arid Ecosystems Using LiDAR, Sentinel-2, GIS Data, and Analysis. Remote Sensing, 2022, 14, 5425. | 1.8 | 5 |
| 74 | Malware Detection by Control-Flow Graph Level Representation Learning With Graph Isomorphism Network. IEEE Access, 2022, 10, 111830-111841. | 2.6 | 5 |
| 75 | Detection of Android Malware Behavior in Browser Downloads. , 2022, , . | | 0 |

| # | Article | IF | Citations |
|---|---|---|---|
| 76 | A comprehensive survey on deep learning based malware detection techniques. Computer Science Review, 2023, 47, 100529. | 10.2 | 36 |
| 77 | Diffusion of White-Hat Botnet Using Lifespan with Controllable Ripple Effect for Malware Removal in IoT Networks. Sensors, 2023, 23, 1018. | 2.1 | 2 |
| 78 | A Review on Nature, Cybercrime and Best Practices of Digital Footprints. , 2022, , . | | 0 |
| 79 | Prior Knowledge based Advanced Persistent Threats Detection for IoT in a Realistic Benchmark. , 2022, , . | | 2 |
| 80 | A Novel and Efficient Sequential Learning-Based Malware Classification Model. , 2022, , . | | 1 |
| 81 | A Blueprint for Collaborative Cybersecurity Operations Centres with Capacity for Shared Situational Awareness, Coordinated Response, and Joint Preparedness. , 2022, , . | | 3 |
| 82 | Study ofÂanÂApproach Based onÂtheÂAnalysis ofÂComputer Program Execution Traces forÂthe Detection ofÂVulnerabilities. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2022, , 105-115. | 0.2 | 0 |
| 83 | A Cheating Attack on a Whitelist-based Anti-Ransomware Solution and its Countermeasure. , 2023, , . | | 2 |
| 84 | Early-Stage Ransomware Detection Based onÂPre-attack Internal API Calls. Lecture Notes in Networks and Systems, 2023, , 417-429. | 0.5 | 0 |
| 85 | TCMal: A Hybrid Deep Learning Model for Encrypted Malicious Traffic Classification. , 2022, , . | | 2 |
| 86 | PDF Malware Detection Based on Fuzzy Unordered Rule Induction Algorithm (FURIA). Applied Sciences (Switzerland), 2023, 13, 3980. | 1.3 | 2 |
| 87 | Study of Various Cyber Threats and Their Mitigation Techniques Requirements. Wireless Personal Communications, 0, , . | 1.8 | 1 |
| 88 | A Survey of Malware Forensics Analysis Techniques and Tools. , 2023, , . | | 1 |
| 89 | Detecting Malware Activities With MalpMiner: A Dynamic Analysis Approach. IEEE Access, 2023, 11, 84772-84784. | 2.6 | 0 |
| 91 | CLOUDOSCOPE: Detecting Anti-Forensic Malware using Public Cloud Environments. , 2023, , . | | 0 |
| 95 | Delving and Unveiling the Malicious World: Implementing Malware Analysis for Preventive Approach. , 2023, , . | | 2 |
| 99 | Malware Analysis and Its Mitigation Tools. Advances in Information Security, Privacy, and Ethics Book Series, 2023, , 263-284. | 0.4 | 2 |
| 100 | PDFalse: Evasive Malicious PDF Machine Learning Classifier. , 2023, , . | | 1 |

| # | Article | IF | Citations |
|---|---|---|---|
| 101 | Machine learning aided malware detection for secure and smart manufacturing: a comprehensive analysis of the state of the art. International Journal on Interactive Design and Manufacturing, 0, , . | 1.3 | 0 |
| 106 | Scaling a Machine Learning Approach to many kinds of Malicious Behavior for Cybersecurity. , 2023, , . | | 0 |
| 107 | Evaluation of Information Technology Equivalence in Telemedicine. , 2023, , . | | 0 |
| 110 | Hide My Payload: An Empirical Study of Antimalware Evasion Tools. , 2023, , . | | 0 |
| 111 | Android Operating System. Progress in IS, 2024, , 25-42. | 0.5 | 0 |
| 112 | Enhancing Android Malware Detection: CFS Based Texture Feature Selection and Ensembled Classifier for Malware App Analysis. Communications in Computer and Information Science, 2024, , 292-306. | 0.4 | 0 |
| 113 | Enhancing Ransomware Detection: A Registry Analysis-Based Approach. , 2023, , . | | 0 |
| 115 | Enhancing Cybersecurity Resilience: Real-time Ransomware Detection using AES Algorithm on Kafka Stream. , 2023, , . | | 0 |