Android HIV: A Study of Repackaging Malware for Evad

IEEE Transactions on Information Forensics and Security
15, 987-1001
DOI: 10.1109/tifs.2019.2932228

Citation Report

#	Article	IF	Citations
1	An Energy-Efficient Cross-Layer-Sensing Clustering Method Based on Intelligent Fog Computing in WSNs. IEEE Access, 2019, 7, 144165-144177.	2.6	27
2	A3CM: Automatic Capability Annotation for Android Malware. IEEE Access, 2019, 7, 147156-147168.	2.6	29
3	Insider Threat Identification Using the Simultaneous Neural Learning of Multi-Source Logs. IEEE Access, 2019, 7, 183162-183176.	2.6	22
4	Using AI to Attack VA: A Stealthy Spyware Against Voice Assistances in Smart Phones. IEEE Access, 2019, 7, 153542-153554.	2.6	11
5	DeepBalance: Deep-Learning and Fuzzy Oversampling for Vulnerability Detection. IEEE Transactions on Fuzzy Systems, 2019, , 1-1.	6.5	50
6	An Efficient Multi-Message and Multi-Receiver Signcryption Scheme for Heterogeneous Smart Mobile IoT. IEEE Access, 2019, 7, 180205-180217.	2.6	27
7	Epidemic Heterogeneity and Hierarchy: A Study of Wireless Hybrid Worm Propagation. IEEE Transactions on Mobile Computing, 2022, 21, 1639-1656.	3.9	5
8	Security and privacy in 6G networks: New areas and new challenges. Digital Communications and Networks, 2020, 6, 281-291.	2.7	206
9	Incentive compatible and anti-compounding of wealth in proof-of-stake. Information Sciences, 2020, 530, 85-94.	4.0	30
10	Privacy-preserving searchable encryption in the intelligent edge computing. Computer Communications, 2020, 164, 31-41.	3.1	13
11	EncodeORE: Reducing Leakage and Preserving Practicality in Order-Revealing Encryption. IEEE Transactions on Dependable and Secure Computing, 2022, 19, 1579-1591.	3.7	15
12	Privacyâ€aware PKI model with strong forward security. International Journal of Intelligent Systems, 2022, 37, 10049-10065.	3.3	16
13	Trustworthy blockchainâ€based medical Internet of thing for minimal invasive surgery training simulator. Concurrency Computation Practice and Experience, 2022, 34, e5816.	1.4	2
14	An Android Inline Hooking Framework for the Securing Transmitted Data. Sensors, 2020, 20, 4201.	2.1	4
15	A botnets control strategy based on variable forgetting rate of control commands. Concurrency Computation Practice and Experience, 2022, 34, e6118.	1.4	1
16	Cyber Resilience in Healthcare Digital Twin on Lung Cancer. IEEE Access, 2020, 8, 201900-201913.	2.6	55
17	Software Vulnerability Analysis and Discovery Using Deep Learning Techniques: A Survey. IEEE Access, 2020, 8, 197158-197172.	2.6	32
18	Adversarial Deep Ensemble: Evasion Attacks and Defenses for Malware Detection. IEEE Transactions on Information Forensics and Security, 2020, 15, 3886-3900.	4.5	76

#	Article	IF	Citations
19	CD-VulD: Cross-Domain Vulnerability Discovery Based on Deep Domain Adaptation. IEEE Transactions on Dependable and Secure Computing, 2022, 19, 438-451.	3.7	28
20	Software Vulnerability Detection Using Deep Neural Networks: A Survey. Proceedings of the IEEE, 2020, 108, 1825-1848.	16.4	214
21	SDCCP: Control the network using softwareâ€defined networking and endâ€toâ€end congestion control. Concurrency Computation Practice and Experience, 2020, , e5716.	1.4	0
22	Code analysis for intelligent cyber systems: A data-driven approach. Information Sciences, 2020, 524, 46-58.	4.0	25
23	Android Malware Family Classification and Analysis: Current Status and Future Directions. Electronics (Switzerland), 2020, 9, 942.	1.8	30
24	FIMPA: A Fixed Identity Mapping Prediction Algorithm in Edge Computing Environment. IEEE Access, 2020, 8, 17356-17365.	2.6	4
25	Secure and Efficient Data Sharing in Dynamic Vehicular Networks. IEEE Internet of Things Journal, 2020, 7, 8208-8217.	5.5	13
26	Secure extended wildcard pattern matching protocol from cut-and-choose oblivious transfer. Information Sciences, 2020, 529, 132-140.	4.0	8
27	Network Topology Inference Using Higher-Order Statistical Characteristics of End-to-End Measured Delays. IEEE Access, 2020, 8, 59960-59975.	2.6	3
28	Adversarial android malware detection for mobile multimedia applications in IoT environments. Multimedia Tools and Applications, 2021, 80, 16713-16729.	2.6	11
29	IDS Intelligent Configuration Scheme Against Advanced Adaptive Attacks. IEEE Transactions on Network Science and Engineering, 2021, 8, 995-1008.	4.1	8
30	Extortion and Cooperation in Rating Protocol Design for Competitive Crowdsourcing. IEEE Transactions on Computational Social Systems, 2021, 8, 246-259.	3.2	8
31	Detection resource allocation scheme for two-layer cooperative IDSs in smart grids. Journal of Parallel and Distributed Computing, 2021, 147, 236-247.	2.7	8
32	Fooling intrusion detection systems using adversarially autoencoder. Digital Communications and Networks, 2021, 7, 453-460.	2.7	20
33	A Performance-Sensitive Malware Detection System Using Deep Learning on Mobile Devices. IEEE Transactions on Information Forensics and Security, 2021, 16, 1563-1578.	4.5	66
34	Towards a physical-world adversarial patch for blinding object detection models. Information Sciences, 2021, 556, 459-471.	4.0	37
35	Daedalus: Breaking Nonmaximum Suppression in Object Detection via Adversarial Examples. IEEE Transactions on Cybernetics, 2022, 52, 7427-7440.	6.2	24
36	AdMat: A CNN-on-Matrix Approach to Android Malware Detection and Classification. IEEE Access, 2021, 9, 39680-39694.	2.6	36

#	Article	IF	Citations
37	The Efficiency of Vulnerability Detection Based on Deep Learning. Advances in Intelligent Systems and Computing, 2021, , 449-455.	0.5	0
38	Deep Learning Based Attack Detection for Cyber-Physical System Cybersecurity: A Survey. IEEE/CAA Journal of Automatica Sinica, 2022, 9, 377-391.	8.5	150
39	Evading Static and Dynamic Android Malware Detection Mechanisms. Communications in Computer and Information Science, 2021, , 33-48.	0.4	1
40	Backdoor Attack on Machine Learning Based Android Malware Detectors. IEEE Transactions on Dependable and Secure Computing, 2022, 19, 3357-3370.	3.7	13
41	PetaDroid: Adaptive Android Malware Detection Using Deep Learning. Lecture Notes in Computer Science, 2021, , 319-340.	1.0	6
42	A Dynamic Robust DL-Based Model for Android Malware Detection. IEEE Access, 2021, 9, 74510-74521.	2.6	20
43	Secure Repackage-Proofing Framework for Android Apps Using Collatz Conjecture. IEEE Transactions on Dependable and Secure Computing, 2022, 19, 3271-3285.	3.7	1
44	An Improved Genetic Algorithm for Safety and Availability Checking in Cyber-Physical Systems. IEEE Access, 2021, 9, 56869-56880.	2.6	2
45	A Survey of Android Malware Detection with Deep Neural Models. ACM Computing Surveys, 2021, 53, 1-36.	16.1	156
46	A comparative study of smartphone and smartwatch apps. , 2021, , .		8
47	Enhanced DNNs for malware classification with GAN-based adversarial training. Journal of Computer Virology and Hacking Techniques, 2021, 17, 153-163.	1.6	16
48	A Review on Android Malware: Attacks, Countermeasures and Challenges Ahead. Journal of Cyber Security and Mobility, 0, , .	0.7	9
49	Smartwatch User Authentication by Sensing Tapping Rhythms and Using One-Class DBSCAN. Sensors, 2021, 21, 2456.	2.1	4
50	Using API Call Sequences for IoT Malware Classification Based on Convolutional Neural Networks. International Journal of Software Engineering and Knowledge Engineering, 2021, 31, 587-612.	0.6	2
51	Robust Android Malware Detection against Adversarial Example Attacks. , 2021, , .		11
52	Malicious application detection in android â€" A systematic literature review. Computer Science Review, 2021, 40, 100373.	10.2	31
53	Android Malware Detection using Function Call Graph with Graph Convolutional Networks. , 2021, , .		5
54	Deep neural-based vulnerability discovery demystified: data, model and performance. Neural Computing and Applications, 2021, 33, 13287-13300.	3.2	12

#	Article	IF	Citations
55	I Want My App That Way: Reclaiming Sovereignty Over Personal Devices. , 2021, , .		10
56	Metamorphic Detection of Repackaged Malware. , 2021, , .		3
57	A Survey on Adversarial Attack in the Age of Artificial Intelligence. Wireless Communications and Mobile Computing, 2021, 2021, 1-22.	0.8	20
58	On machine learning effectiveness for malware detection in Android OS using static analysis data. Journal of Information Security and Applications, 2021, 59, 102794.	1.8	23
59	Software engineering techniques for statically analyzing mobile apps: research trends, characteristics, and potential for industrial adoption. Journal of Internet Services and Applications, 2021, 12, .	1.6	1
60	Hybrid sequenceâ€based Android malware detection using natural language processing. International Journal of Intelligent Systems, 2021, 36, 5770-5784.	3.3	45
61	HomDroid: detecting Android covert malware by social-network homophily analysis. , 2021, , .		10
62	Addressing Overfitting Problem in Deep Learning-Based Solutions for Next Generation Data-Driven Networks. Wireless Communications and Mobile Computing, 2021, 2021, 1-10.	0.8	9
63	Kalman prediction-based virtual network experimental platform for smart living. Computer Communications, 2021, 177, 156-165.	3.1	1
64	Android malware detection via an app similarity graph. Computers and Security, 2021, 109, 102386.	4.0	24
65	Secure boot, trusted boot and remote attestation for ARM TrustZone-based IoT Nodes. Journal of Systems Architecture, 2021, 119, 102240.	2.5	15
66	Malicious mining code detection based on ensemble learning in cloud computing environment. Simulation Modelling Practice and Theory, 2021, 113, 102391.	2.2	38
67	Malware Classification Based on Multilayer Perception and Word2Vec for IoT Security. ACM Transactions on Internet Technology, 2022, 22, 1-22.	3.0	14
68	DL-FHMC: Deep Learning-Based Fine-Grained Hierarchical Learning Approach for Robust Malware Classification. IEEE Transactions on Dependable and Secure Computing, 2022, 19, 3432-3447.	3.7	15
69	Active Warden Attack: On the (In)Effectiveness of Android App Repackage-Proofing. IEEE Transactions on Dependable and Secure Computing, 2022, 19, 3508-3520.	3.7	4
70	Unsupervised Insider Detection Through Neural Feature Learning and Model Optimisation. Lecture Notes in Computer Science, 2019, , 18-36.	1.0	5
71	Classification of IoT Malware based on Convolutional Neural Network. , 2020, , .		2
72	From Image to Code. , 2020, , .		5

#	Article	IF	Citations
73	Few-shot relation classification by context attention-based prototypical networks with BERT. Eurasip Journal on Wireless Communications and Networking, 2020, 2020, .	1.5	11
74	Constrained Adversarial Attacks Against Image-Based Malware Classification System. Communications in Computer and Information Science, 2021, , 198-208.	0.4	0
75	LCHI: Low-Order Correlation and High-Order Interaction Integrated Model Oriented to Network Intrusion Detection. Wireless Communications and Mobile Computing, 2021, 2021, 1-16.	0.8	1
76	Android application forensics: A survey of obfuscation, obfuscation detection and deobfuscation techniques and their impact on investigations. Forensic Science International: Digital Investigation, 2021, 39, 301285.	1.2	13
77	A Robust Malware Detection Approach for Android System Against Adversarial Example Attacks. , 2019, , .		8
78	Robust Android Malware Detection Based on Attributed Heterogenous Graph Embedding. Communications in Computer and Information Science, 2020, , 432-446.	0.4	1
79	An Empirical Study of Code Deobfuscations on Detecting Obfuscated Android Piggybacked Apps. , 2020, , .		3
80	Recent Advances in Android Mobile Malware Detection: A Systematic Literature Review. IEEE Access, 2021, 9, 146318-146349.	2.6	9
81	Domain adaptation for Windows advanced persistent threat detection. Computers and Security, 2022, 112, 102496.	4.0	12
82	A Green Stackelberg-game Incentive Mechanism for Multi-service Exchange in Mobile Crowdsensing. ACM Transactions on Internet Technology, 2022, 22, 1-29.	3.0	9
83	Evasion Is Not Enough: A Case Study ofÂAndroid Malware. Lecture Notes in Computer Science, 2020, , 167-174.	1.0	6
84	CAVAEva: An Engineering Platform forÂEvaluating Commercial Anti-malware Applications on Smartphones. Lecture Notes in Computer Science, 2020, , 208-224.	1.0	0
85	DroidAutoML: A Microservice Architecture to Automate the Evaluation of Android Machine Learning Detection Systems. Lecture Notes in Computer Science, 2020, , 148-165.	1.0	1
86	Dynamic redirection of real-time data streams for elastic stream computing. Future Generation Computer Systems, 2020, 112, 193-208.	4.9	6
87	DroidEnemy: Battling adversarial example attacks for Android malware detection. Digital Communications and Networks, 2022, 8, 1040-1047.	2.7	11
88	A Context-Aware Neural Embedding for Function-Level Vulnerability Detection. Algorithms, 2021, 14, 335.	1.2	8
89	Structural Attack against Graph Based Android Malware Detection. , 2021, , .		14
90	Image Speckle Denoising for Securing Internet of Smart Sensors. Security and Communication Networks, 2021, 2021, 1-10.	1.0	1

#	Article	IF	Citations
91	Adversarial Machine Learning: A Multilayer Review of the State-of-the-Art and Challenges for Wireless and Mobile Systems. IEEE Communications Surveys and Tutorials, 2022, 24, 123-159.	24.8	21
92	Mu-Net: Multi-Path Upsampling Convolution Network for Medical Image Segmentation. CMES - Computer Modeling in Engineering and Sciences, 2022, 131, 73-95.	0.8	7
93	RanSAP: An open dataset of ransomware storage access patterns for training machine learning models. Forensic Science International: Digital Investigation, 2022, 40, 301314.	1.2	16
94	Feature-Based Adversarial Attacks Against Machine Learnt Mobile Malware Detectors. , 2020, , .		0
95	Crystal Ball: From Innovative Attacks to Attack Effectiveness Classifier. IEEE Access, 2022, 10, 1317-1333.	2.6	1
96	Digital Twin forÂCybersecurity: Towards Enhancing Cyber Resilience. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2022, , 57-76.	0.2	5
97	Deep Neural Embedding for Software Vulnerability Discovery: Comparison and Optimization. Security and Communication Networks, 2022, 2022, 1-12.	1.0	13
98	Failure-Tolerant Monitoring Based on Spatialâ€“Temporal Correlation via Mobile Sensors for Large-Scale Acyclic Flow Systems in Smart Cities. IEEE Internet of Things Journal, 2022, 9, 19561-19574.	5.5	0
100	Self-Learning Spatial Distribution-Based Intrusion Detection for Industrial Cyber-Physical Systems. IEEE Transactions on Computational Social Systems, 2022, 9, 1693-1702.	3.2	12
101	Intelligent Malware Defenses. Lecture Notes in Computer Science, 2022, , 217-253.	1.0	2
102	Design and Formal Analysis of a Lightweight MIPv6 Authentication Scheme. IEEE Internet of Things Journal, 2022, 9, 19238-19245.	5.5	3
103	Eavesdropping user credentials via GPU side channels on smartphones. , 2022, , .		4
104	<scp>Powerâ€efficient</scp> optimized clustering method with intelligent fog computing for wireless sensor network<scp>s</scp>. Concurrency Computation Practice and Experience, 2022, 34, .	1.4	0
105	Intelligent detection of vulnerable functions in software through neural embeddingâ€based code analysis. International Journal of Network Management, 2023, 33, .	1.4	4
106	Less Is More: Robust and Novel Features for Malicious Domain Detection. Electronics (Switzerland), 2022, 11, 969.	1.8	5
107	AndroCreme: Unseen Android Malware Detection Based on Inductive Conformal Learning. , 2021, , .		1
108	A First Look at Security Risks of Android TV Apps. , 2021, , .		3
109	Secure medical digital twin via human-centric interaction and cyber vulnerability resilience. Connection Science, 2022, 34, 895-910.	1.8	18

#	Article	IF	Citations
110	Cyber Code Intelligence for Android Malware Detection. IEEE Transactions on Cybernetics, 2023, 53, 617-627.	6.2	12
111	MsDroid: Identifying Malicious Snippets for Android Malware Detection. IEEE Transactions on Dependable and Secure Computing, 2023, 20, 2025-2039.	3.7	8
112	TSDroid: A Novel Android Malware Detection Framework Based on Temporal & Spatial Metrics in IoMT. ACM Transactions on Sensor Networks, 2023, 19, 1-23.	2.3	3
113	Investigating the impact of vulnerability datasets on deep learning-based vulnerability detectors. PeerJ Computer Science, 0, 8, e975.	2.7	3
114	ShadowDroid: Practical Black-box Attack against ML-based Android Malware Detection. , 2021, , .		4
115	Adversarial malware sample generation method based on the prototype of deep learning detector. Computers and Security, 2022, 119, 102762.	4.0	6
116	Arms Race in Adversarial Malware Detection: A Survey. ACM Computing Surveys, 2023, 55, 1-35.	16.1	12
117	Deep Learning for Android Malware Defenses: A Systematic Literature Review. ACM Computing Surveys, 2023, 55, 1-36.	16.1	24
118	Mitigating Malicious Adversaries Evasion Attacks in Industrial Internet of Things. IEEE Transactions on Industrial Informatics, 2023, 19, 960-968.	7.2	5
119	A Systematic Overview of the Machine Learning Methods for Mobile Malware Detection. Security and Communication Networks, 2022, 2022, 1-20.	1.0	5
120	FCâ€ACGANâ€based data augmentation for terahertz timeâ€domain spectral concealed hazardous materials identification. International Journal of Intelligent Systems, 0, , .	3.3	0
121	Event detection in online social network: Methodologies, state-of-art, and evolution. Computer Science Review, 2022, 46, 100500.	10.2	16
122	Evaluating Membership Inference Through Adversarial Robustness. Computer Journal, 2022, 65, 2969-2978.	1.5	4
123	Evading Machine-Learning-Based Android Malware Detector for IoT Devices. IEEE Systems Journal, 2023, 17, 2745-2755.	2.9	1
124	TraceDroid: Detecting Android Malware byÂTrace ofÂPrivacy Leakage. Lecture Notes in Computer Science, 2022, , 466-478.	1.0	0
125	Toward Personalized Federated Learning Via Group Collaboration in IIoT. IEEE Transactions on Industrial Informatics, 2023, 19, 8923-8932.	7.2	5
126	Active Learning Based Adversary Evasion Attacks Defense for Malwares in the Internet of Things. IEEE Systems Journal, 2023, 17, 2434-2444.	2.9	3
127	Android Malware Classification by CNN-LSTM. , 2022, , .		3

#	Article	IF	Citations
128	The application of neural network for software vulnerability detection: a review. Neural Computing and Applications, 2023, 35, 1279-1301.	3.2	2
129	Droid-MCFG: Android malware detection system using manifest and control flow traces with multi-head temporal convolutional network. Physical Communication, 2023, 57, 101975.	1.2	4
130	Automated Binary Analysis: A Survey. Lecture Notes in Computer Science, 2023, , 392-411.	1.0	2
131	Effective of Obfuscated Android Malware Detection using Static Analysis. , 2022, , .		1
132	Combining AST Segmentation andÂDeep Semantic Extraction forÂFunction Level Vulnerability Detection. Lecture Notes on Data Engineering and Communications Technologies, 2023, , 93-100.	0.5	0
133	Detecting vulnerabilities in IoT software: New hybrid model and comprehensive data analysis. Journal of Information Security and Applications, 2023, 74, 103467.	1.8	1
134	Hybrid KD-NFT: A multi-layered NFT assisted robust Knowledge Distillation framework for Internet of Things. Journal of Information Security and Applications, 2023, 75, 103483.	1.8	0
135	A Machine Learning Framework for Automatic Detection of Malware. Communications in Computer and Information Science, 2022, , 83-95.	0.4	1
136	DroidHook: a novel API-hook based Android malware dynamic analysis sandbox. Automated Software Engineering, 2023, 30, .	2.2	2
137	Android Ransomware Detection Toolkit. , 2022, , .		0
138	Backdoor attacks against distributed swarm learning. ISA Transactions, 2023, 141, 59-72.	3.1	3
139	Mitigating Malware Attacks using Machine Learning: A Review. , 2023, , .		0
140	A Novel Knowledge Distillation Framework with Intermediate Loss for Android Malware Detection. , 2022, , .		0
141	The Age of Ransomware: A Survey on the Evolution, Taxonomy, and Research Directions. IEEE Access, 2023, 11, 40698-40723.	2.6	9
142	Privacy preserving federated learning for full heterogeneity. ISA Transactions, 2023, 141, 73-83.	3.1	1
143	Machine Learning Based Power Efficient Optimized Communication Ensemble Model with Intelligent Fog Computing for WSNs. Wireless Personal Communications, 2023, 131, 415-429.	1.8	0
144	SVScanner: Detecting smart contract vulnerabilities via deep semantic extraction. Journal of Information Security and Applications, 2023, 75, 103484.	1.8	2
152	â€˜We are adults and deserve control of our phonesâ€™: Examining the risks and opportunities of a right to repair for mobile apps. , 2023, , .		1

#	Article	IF	Citations
156	RGDroid: Detecting Android Malware with Graph Convolutional Networks against Structural Attacks. , 2023, , .		0
162	Characterizing the Use of Code Obfuscation in Malicious and Benign Android Apps. , 2023, , .		0
167	Minimum Selection Feature Importance Guided Attack. , 2023, , .		0
168	A Method for Summarizing and Classifying Evasive Malware. , 2023, , .		0
169	Comprehensive Analysis and Remediation of Insecure Direct Object References (IDOR) Vulnerabilities in Android APIs. , 2023, , .		0
174	On the effectiveness of transferability of adversarial Android malware samples against learning-based detectors. , 2023, , .		0
178	A Comprehensive Study of Learning-based Android Malware Detectors under Challenging Environments. , 2024, , .		0
181	Analysis of android malware detection using machine learning techniques. AIP Conference Proceedings, 2024, , .	0.3	0