

# Mark Stamp

## List of Publications by Year in descending order

Source: <https://exaly.com/author-pdf/4217161/publications.pdf>

Version: 2024-02-01

88  
papers

2,545  
citations

304743

22  
h-index

243625

44  
g-index

94  
all docs

94  
docs citations

94  
times ranked

1100  
citing authors

#	ARTICLE	IF	CITATIONS
1	A comparison of static, dynamic, and hybrid analysis for malware detection. Journal of Computer Virology and Hacking Techniques, 2017, 13, 1-12.	2.2	270
2	Hunting for metamorphic engines. Journal in Computer Virology, 2006, 2, 211-229.	1.9	195
3	An algorithm for the k-error linear complexity of binary sequences with period $2/\sup n/$ . IEEE Transactions on Information Theory, 1993, 39, 1398-1401.	2.4	138
4	Opcode graph similarity and metamorphic detection. Journal in Computer Virology, 2012, 8, 37-52.	1.9	128
5	Structural entropy and metamorphic malware. Journal of Computer Virology and Hacking Techniques, 2013, 9, 179-192.	2.2	105
6	Hunting for undetectable metamorphic viruses. Journal in Computer Virology, 2011, 7, 201-214.	1.9	98
7	Profile hidden Markov models and metamorphic virus detection. Journal in Computer Virology, 2009, 5, 151-169.	1.9	81
8	Hidden Markov models for malware classification. Journal of Computer Virology and Hacking Techniques, 2015, 11, 59-73.	2.2	78
9	Deriving common malware behavior through graph clustering. Computers and Security, 2013, 39, 419-430.	6.0	69
10	Chi-squared distance and metamorphic virus detection. Journal of Computer Virology and Hacking Techniques, 2013, 9, 1-14.	2.2	68
11	Metamorphic worm that carries its own morphing engine. Journal of Computer Virology and Hacking Techniques, 2013, 9, 49-58.	2.2	57
12	Exploring Hidden Markov Models for Virus Analysis: A Semantic Approach. , 2013, , .		55
13	Simple substitution distance and metamorphic detection. Journal of Computer Virology and Hacking Techniques, 2013, 9, 159-170.	2.2	53
14	Feature analysis of encrypted malicious traffic. Expert Systems With Applications, 2019, 125, 130-141.	7.6	53
15	Detecting malware evolution using support vector machines. Expert Systems With Applications, 2020, 143, 113022.	7.6	52
16	Transfer Learning for Image-based Malware Classification. , 2019, , .		46
17	Introduction to Machine Learning with Applications in Information Security. , 0, , .		40
18	Static and Dynamic Analysis of Android Malware. , 2017, , .		40

#	ARTICLE	IF	CITATIONS
19	Convolutional neural networks and extreme learning machines for malware classification. Journal of Computer Virology and Hacking Techniques, 2020, 16, 229-244.	2.2	39
20	Risks of monoculture. Communications of the ACM, 2004, 47, 120.	4.5	38
21	Clustering for malware classification. Journal of Computer Virology and Hacking Techniques, 2017, 13, 95-107.	2.2	37
22	Image spam analysis and detection. Journal of Computer Virology and Hacking Techniques, 2018, 14, 39-52.	2.2	37
23	Deep Learning versus Gist Descriptors for Image-based Malware Classification. , 2018, , .		34
24	Eigenvalue analysis for metamorphic detection. Journal of Computer Virology and Hacking Techniques, 2014, 10, 53-65.	2.2	33
25	Support vector machines and malware detection. Journal of Computer Virology and Hacking Techniques, 2016, 12, 203-212.	2.2	32
26	HTTP attack detection using n-gram analysis. Computers and Security, 2014, 45, 242-254.	6.0	29
27	Masquerade detection using profile hidden Markov models. Computers and Security, 2011, 30, 732-747.	6.0	27
28	Dueling hidden Markov models for virus analysis. Journal of Computer Virology and Hacking Techniques, 2015, 11, 103-118.	2.2	21
29	Hunting for metamorphic JavaScript malware. Journal of Computer Virology and Hacking Techniques, 2015, 11, 89-102.	2.2	20
30	Singular value decomposition and metamorphic detection. Journal of Computer Virology and Hacking Techniques, 2015, 11, 203-216.	2.2	18
31	Clustering versus SVM for malware detection. Journal of Computer Virology and Hacking Techniques, 2016, 12, 213-224.	2.2	16
32	Hidden Markov models with random restarts versus boosting for malware detection. Journal of Computer Virology and Hacking Techniques, 2019, 15, 97-107.	2.2	15
33	A highly metamorphic virus generator. International Journal of Multimedia Intelligence and Security, 2010, 1, 402.	0.1	14
34	Efficient Cryptanalysis of Homophonic Substitution Ciphers. Cryptologia, 2013, 37, 250-281.	0.5	14
35	A Dynamic Heuristic Method for Detecting Packed Malware Using Naive Bayes. , 2019, , .		14
36	An Empirical Analysis of Image-Based Learning Techniques for Malware Classification. , 2021, , 411-435.		14

#	ARTICLE	IF	CITATIONS
37	Compression-based analysis of metamorphic malware. International Journal of Security and Networks, 2015, 10, 124.	0.2	13
38	Classic cryptanalysis using hidden Markov models. Cryptologia, 2017, 41, 1-28.	0.5	13
39	Convolutional neural networks for image spam detection. Information Security Journal, 2020, 29, 103-117.	1.9	13
40	Malware classification with Word2Vec, HMM2Vec, BERT, and ELMo. Journal of Computer Virology and Hacking Techniques, 2023, 19, 1-16.	2.2	13
41	An analysis of Android adware. Journal of Computer Virology and Hacking Techniques, 2019, 15, 147-160.	2.2	12
42	Metamorphic code generation from LLVM bytecode. Journal of Computer Virology and Hacking Techniques, 2014, 10, 177-187.	2.2	11
43	iPhone Security Analysis. Journal of Information Security, 2010, 01, 74-87.	0.8	11
44	Hidden Markov Models for Software Piracy Detection. Information Security Journal, 2013, 22, 140-149.	1.9	10
45	Multifamily malware models. Journal of Computer Virology and Hacking Techniques, 2020, 16, 79-92.	2.2	10
46	An agent-based privacy-enhancing model. Information Management and Computer Security, 2008, 16, 305-319.	1.2	9
47	Hunting for Pirated Software Using Metamorphic Analysis. Information Security Journal, 2014, 23, 68-85.	1.9	9
48	Malware Classification using Long Short-term Memory Models. , 2021, , .		9
49	Static Analysis of Malicious Java Applets. , 2016, , .		8
50	A Survey of Machine Learning Algorithms and Their Application in Information Security. Computer Communications and Networks, 2018, , 33-55.	0.8	8
51	Risks of digital rights management. Communications of the ACM, 2002, 45, 120.	4.5	7
52	Detecting Encrypted and Polymorphic Malware Using Hidden Markov Models. Computer Communications and Networks, 2018, , 281-299.	0.8	7
53	Computer-aided diagnosis of low grade endometrial stromal sarcoma (LGESS). Computers in Biology and Medicine, 2021, 138, 104874.	7.0	7
54	A Comparative Analysis of Android Malware. , 2019, , .		7

#	ARTICLE	IF	CITATIONS
55	SIGABA: Cryptanalysis of the Full Keyspace. <i>Cryptologia</i> , 2007, 31, 201-222.	0.5	6
56	Automating NFC message sending for good and evil. <i>Journal of Computer Virology and Hacking Techniques</i> , 2014, 10, 273-297.	2.2	5
57	Malware Classification with Word Embedding Features. , 2021, , .		5
58	Malware Classification with GMM-HMM Models. , 2021, , .		5
59	A Comparison of Word2Vec, HMM2Vec, and PCA2Vec for Malware Classification. , 2021, , 287-320.		5
60	Acoustic Gait Analysis using Support Vector Machines. , 2018, , .		5
61	Sentiment Analysis for Troll Detection on Weibo. , 2021, , 555-579.		5
62	P3P privacy enhancing agent. , 2006, , .		4
63	Masquerade detection on GUI-based Windows systems. <i>International Journal of Security and Networks</i> , 2015, 10, 32.	0.2	4
64	VigenÃre scores for malware detection. <i>Journal of Computer Virology and Hacking Techniques</i> , 2018, 14, 157-165.	2.2	4
65	Black box analysis of android malware detectors. <i>Array</i> , 2020, 6, 100022.	4.0	4
66	Support Vector Machines for Image Spam Analysis. , 2018, , .		4
67	Cluster Analysis of Malware Family Relationships. , 2021, , 361-379.		4
68	On Ensemble Learning. , 2021, , 223-246.		4
69	Function Call Graphs Versus Machine Learning for Malware Detection. <i>Computer Communications and Networks</i> , 2018, , 259-279.	0.8	3
70	A New Dataset for Smartphone Gesture-based Authentication. , 2021, , .		3
71	Autocorrelation Analysis of Financial Botnet Traffic. , 2018, , .		3
72	On the Effectiveness of Generic Malware Models. , 2018, , .		3

#	ARTICLE	IF	CITATIONS
73	Solvable problems in enterprise digital rights management. Information Management and Computer Security, 2007, 15, 33-45.	1.2	2
74	A completely covert audio channel in Android. Journal of Computer Virology and Hacking Techniques, 2017, 13, 141-152.	2.2	2
75	On the Effectiveness of Generic Malware Models. , 2018, , .		2
76	Robust Hashing for Image-based Malware Classification. , 2018, , .		2
77	Word Embedding Techniques for Malware Evolution Detection. , 2021, , 321-343.		2
78	Emulation Versus Instrumentation for Android Malware Detection. Advanced Sciences and Technologies for Security Applications, 2021, , 1-20.	0.5	2
79	Cryptanalysis of Typex. Cryptologia, 2014, 38, 116-132.	0.5	1
80	Advanced transcriptase for JavaScript malware. , 2016, , .		1
81	Robust Hashing for Image-based Malware Classification. , 2018, , .		1
82	A Selective Survey of Deep Learning Techniques and Their Application to Malware Analysis. , 2021, , 3-51.		1
83	Circular Binary Sequences. SIAM Review, 1992, 34, 496-497.	9.5	0
84	BootBandit: A macOS bootloader attack. Engineering Reports, 2019, 1, e12032.	1.7	0
85	A characterization of a class of discrete nonlinear feedback systems. Communications in Information and Systems, 2005, 5, 305-310.	0.5	0
86	SocioBot: a Twitter-based botnet. International Journal of Security and Networks, 2017, 12, 1.	0.2	0
87	Universal Adversarial Perturbations and Image Spam Classifiers. , 2021, , 633-651.		0
88	Machine Learning for Malware Evolution Detection. Advances in Information Security, 2022, , 183-213.	1.2	0