Mamoru Mimura

List of Publications by Year
in descending order

41	301	933264 10	1058333 14
papers	citations	h-index	g-index

41	41	41	69
all docs	docs citations	times ranked	citing authors

#	Article	IF	Citations
1	Applying NLP techniques to malware detection in a practical environment. International Journal of Information Security, 2022, 21, 279-291.	2.3	17
2	On the Possibility of Evasion Attacks with Macro Malware. Advances in Intelligent Systems and Computing, 2022, , 43-59.	0.5	3
3	Toward Automated Audit of Client-Side Vulnerability Against Cross-Site Scripting. Lecture Notes in Networks and Systems, 2022, , 148-157.	0.5	1
4	Evaluation of printable character-based malicious PE file-detection method. Internet of Things (Netherlands), 2022, 19, 100521.	4.9	6
5	Automating post-exploitation with deep reinforcement learning. Computers and Security, 2021, 100, 102108.	4.0	36
6	Detection of malicious javascript on an imbalanced dataset. Internet of Things (Netherlands), 2021, 13, 100357.	4.9	15
7	Static detection of malicious PowerShell based on word embeddings. Internet of Things (Netherlands), 2021, 15, 100404.	4.9	14
8	Oversampling for Detection of Malicious JavaScript in Realistic Environment. Lecture Notes in Networks and Systems, 2021, , 176-187.	0.5	1
9	Data augmentation of JavaScript dataset using DCGAN and random seed. , 2021, , .		3
10	Adjusting lexical features of actual proxy logs for intrusion detection. Journal of Information Security and Applications, 2020, 50, 102408.	1.8	9
11	Using fake text vectors to improve the sensitivity of minority class for macro malware detection. Journal of Information Security and Applications, 2020, 54, 102600.	1.8	13
12	An Improved Method of Detecting Macro Malware on an Imbalanced Dataset. IEEE Access, 2020, 8, 204709-204717.	2.6	15
13	o-glasses: Visualizing X86 Code From Binary Using a 1D-CNN. IEEE Access, 2020, 8, 31753-31763.	2.6	3
14	o-glassesX: Compiler Provenance Recovery with Attention Mechanism from a Short Code Fragment. , 2020, , .		10
15	Detection of Malicious PowerShell Using Word-Level Language Models. Lecture Notes in Computer Science, 2020, , 39-56.	1.0	4
16	Using LSI to Detect Unknown Malicious VBA Macros. Journal of Information Processing, 2020, 28, 493-501.	0.3	8
17	Detecting Unknown Malware from ASCII Strings with Natural Language Processing Techniques. , 2019, , .		5
18	Filtering Malicious JavaScript Code with Doc2Vec on an Imbalanced Dataset. , 2019, , .		12

#	Article	IF	Citations
19	Detecting Unseen Malicious VBA Macros with NLP Techniques. Journal of Information Processing, 2019, 27, 555-563.	0.3	10
20	Analysis of Division Property using MILP Method for Lightweight Blockcipher Piccolo. , 2019, , .		1
21	An Analysis of TCP ACK Storm DoS Attack on Virtual Network. , 2019, , .		1
22	Towards Efficient Detection of Malicious VBA Macros with LSI. Lecture Notes in Computer Science, 2019, , 168-185.	1.0	11
23	An Attempt to Read Network Traffic with Doc2vec. Journal of Information Processing, 2019, 27, 711-719.	0.3	5
24	Using Sparse Composite Document Vectors to Classify VBA Macros. Lecture Notes in Computer Science, 2019, , 714-720.	1.0	4
25	Reading Network Packets as a Natural Language for Intrusion Detection. Lecture Notes in Computer Science, 2018, , 339-350.	1.0	9
26	Verifiable Secret Sharing Scheme Using Hash Values. , 2018, , .		8
27	Leaving All Proxy Server Logs to Paragraph Vector. Journal of Information Processing, 2018, 26, 804-812.	0.3	9
28	Discovering New Malware Families Using a Linguistic-Based Macros Detection Method. , 2018, , .		4
29	Slow-Port-Exhaustion DoS Attack on Virtual Network Using Port Address Translation. , 2018, , .		1
30	On the Effectiveness of Extracting Important Words from Proxy Logs. , 2018, , .		0
31	A Linguistic Approach Towards Intrusion Detection in Actual Proxy Logs. Lecture Notes in Computer Science, 2018, , 708-718.	1.0	5
32	Macros Finder: Do You Remember LOVELETTER?. Lecture Notes in Computer Science, 2018, , 3-18.	1.0	11
33	Abusing TCP Retransmission for DoS Attack Inside Virtual Network. Lecture Notes in Computer Science, 2018, , 199-211.	1.0	3
34	A Practical Experiment of the HTTP-Based RAT Detection Method in Proxy Server Logs. , 2017, , .		10
35	Dark Domain Name Attack: A New Threat toÂDomain Name System. Lecture Notes in Computer Science, 2017, , 405-414.	1.0	1
36	Heavy Log Reader: Learning the Context ofÂCyber Attacks Automatically withÂParagraphÂVector. Lecture Notes in Computer Science, 2017, , 146-163.	1.0	11

#	Article	IF	Citations
37	Leveraging Man-in-the-middle DoS Attack withÂInternal TCP Retransmissions inÂVirtualÂNetwork. Lecture Notes in Computer Science, 2017, , 367-386.	1.0	2
38	Long-Term Performance of a Generic Intrusion Detection Method Using Doc2vec. , 2017, , .		5
39	Is Emulating "Binary Grep in Eyes" Possible with Machine Learning?. , 2017, , .		2
40	Evaluation of a Brute Forcing Tool that Extracts the RAT from a Malicious Document File. , 2016, , .		10
41	Behavior Shaver: An Application Based Layer 3 VPN that Conceals Traffic Patterns Using SCTP. , 2010, , .		3