

Mamoru Mimura

List of Publications by Year in descending order

Source: <https://exaly.com/author-pdf/9251793/publications.pdf>

Version: 2024-02-01

41
papers

301
citations

933264

10
h-index

1058333

14
g-index

41
all docs

41
docs citations

41
times ranked

69
citing authors

#	ARTICLE	IF	CITATIONS
1	Automating post-exploitation with deep reinforcement learning. Computers and Security, 2021, 100, 102108.	4.0	36
2	Applying NLP techniques to malware detection in a practical environment. International Journal of Information Security, 2022, 21, 279-291.	2.3	17
3	An Improved Method of Detecting Macro Malware on an Imbalanced Dataset. IEEE Access, 2020, 8, 204709-204717.	2.6	15
4	Detection of malicious javascript on an imbalanced dataset. Internet of Things (Netherlands), 2021, 13, 100357.	4.9	15
5	Static detection of malicious PowerShell based on word embeddings. Internet of Things (Netherlands), 2021, 15, 100404.	4.9	14
6	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
7	Filtering Malicious JavaScript Code with Doc2Vec on an Imbalanced Dataset. , 2019, , .		12
8	Heavy Log Reader: Learning the Context of Cyber Attacks Automatically with Paragraph Vector. Lecture Notes in Computer Science, 2017, , 146-163.	1.0	11
9	Towards Efficient Detection of Malicious VBA Macros with LSI. Lecture Notes in Computer Science, 2019, , 168-185.	1.0	11
10	Macros Finder: Do You Remember LOVELETTER?. Lecture Notes in Computer Science, 2018, , 3-18.	1.0	11
11	Evaluation of a Brute Forcing Tool that Extracts the RAT from a Malicious Document File. , 2016, , .		10
12	A Practical Experiment of the HTTP-Based RAT Detection Method in Proxy Server Logs. , 2017, , .		10
13	Detecting Unseen Malicious VBA Macros with NLP Techniques. Journal of Information Processing, 2019, 27, 555-563.	0.3	10
14	o-glassesX: Compiler Provenance Recovery with Attention Mechanism from a Short Code Fragment. , 2020, , .		10
15	Reading Network Packets as a Natural Language for Intrusion Detection. Lecture Notes in Computer Science, 2018, , 339-350.	1.0	9
16	Leaving All Proxy Server Logs to Paragraph Vector. Journal of Information Processing, 2018, 26, 804-812.	0.3	9
17	Adjusting lexical features of actual proxy logs for intrusion detection. Journal of Information Security and Applications, 2020, 50, 102408.	1.8	9
18	Verifiable Secret Sharing Scheme Using Hash Values. , 2018, , .		8

#	ARTICLE	IF	CITATIONS
19	Using LSI to Detect Unknown Malicious VBA Macros. Journal of Information Processing, 2020, 28, 493-501.	0.3	8
20	Evaluation of printable character-based malicious PE file-detection method. Internet of Things (Netherlands), 2022, 19, 100521.	4.9	6
21	Long-Term Performance of a Generic Intrusion Detection Method Using Doc2vec. , 2017, , .		5
22	A Linguistic Approach Towards Intrusion Detection in Actual Proxy Logs. Lecture Notes in Computer Science, 2018, , 708-718.	1.0	5
23	Detecting Unknown Malware from ASCII Strings with Natural Language Processing Techniques. , 2019, , .		5
24	An Attempt to Read Network Traffic with Doc2vec. Journal of Information Processing, 2019, 27, 711-719.	0.3	5
25	Discovering New Malware Families Using a Linguistic-Based Macros Detection Method. , 2018, , .		4
26	Using Sparse Composite Document Vectors to Classify VBA Macros. Lecture Notes in Computer Science, 2019, , 714-720.	1.0	4
27	Detection of Malicious PowerShell Using Word-Level Language Models. Lecture Notes in Computer Science, 2020, , 39-56.	1.0	4
28	Behavior Shaver: An Application Based Layer 3 VPN that Conceals Traffic Patterns Using SCTP. , 2010, , .		3
29	o-glasses: Visualizing X86 Code From Binary Using a 1D-CNN. IEEE Access, 2020, 8, 31753-31763.	2.6	3
30	On the Possibility of Evasion Attacks with Macro Malware. Advances in Intelligent Systems and Computing, 2022, , 43-59.	0.5	3
31	Abusing TCP Retransmission for DoS Attack Inside Virtual Network. Lecture Notes in Computer Science, 2018, , 199-211.	1.0	3
32	Data augmentation of JavaScript dataset using DCGAN and random seed. , 2021, , .		3
33	Leveraging Man-in-the-middle DoS Attack with Internal TCP Retransmissions in Virtual Network. Lecture Notes in Computer Science, 2017, , 367-386.	1.0	2
34	Is Emulating "Binary Grep in Eyes" Possible with Machine Learning?. , 2017, , .		2
35	Dark Domain Name Attack: A New Threat to Domain Name System. Lecture Notes in Computer Science, 2017, , 405-414.	1.0	1
36	Slow-Port-Exhaustion DoS Attack on Virtual Network Using Port Address Translation. , 2018, , .		1

#	ARTICLE	IF	CITATIONS
37	Analysis of Division Property using MILP Method for Lightweight Blockcipher Piccolo. , 2019, , .		1
38	An Analysis of TCP ACK Storm DoS Attack on Virtual Network. , 2019, , .		1
39	Toward Automated Audit of Client-Side Vulnerability Against Cross-Site Scripting. Lecture Notes in Networks and Systems, 2022, , 148-157.	0.5	1
40	Oversampling for Detection of Malicious JavaScript in Realistic Environment. Lecture Notes in Networks and Systems, 2021, , 176-187.	0.5	1
41	On the Effectiveness of Extracting Important Words from Proxy Logs. , 2018, , .		0