Daiki Chiba

List of Publications by Year
in descending order

Source: https://exaly.com/author-pdf/6000109/publications.pdf

Version: 2024-02-01

36 papers	302 citations	1937685 4 h-index	1372567 10 g-index
36 all docs	36 docs citations	36 times ranked	195 citing authors

#	Article	IF	Citations
1	DomainPrio: Prioritizing Domain Name Investigations to Improve SOC Efficiency. IEEE Access, 2022, 10, 34352-34368.	4.2	0
2	Understanding the Fake Removal Information Advertisement Sites. Journal of Information Processing, 2021, 29, 392-405.	0.4	1
3	A Comprehensive Measurement of Cloud Service Abuse. Journal of Information Processing, 2021, 29, 93-102.	0.4	0
4	To Get Lost is to Learn the Way: An Analysis of Multi-Step Social Engineering Attacks on the Web. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2021, E104.A, 162-181.	0.3	2
5	A First Look at COVID-19 Domain Names: Origin and Implications. Lecture Notes in Computer Science, 2021, , 39-53.	1.3	2
6	Analyzing Security Risks of Ad-Based URL Shortening Services Caused by Usersâ€™ Behaviors. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2021, , 3-22.	0.3	2
7	A Large-scale Analysis of Cloud Service Abuse. , 2020, , .		2
8	Detecting Malware-infected Hosts Using Templates of Multiple HTTP Requests. , 2020, , .		3
9	Exploration into Gray Area: Toward Efficient Labeling for Detecting Malicious Domain Names. IEICE Transactions on Communications, 2020, E103.B, 375-388.	0.7	2
10	DomainScouter: Analyzing the Risks of Deceptive Internationalized Domain Names. IEICE Transactions on Information and Systems, 2020, E103.D, 1493-1511.	0.7	3
11	Time-Series Measurement of Parked Domain Names. , 2020, , .		2
12	It Never Rains but It Pours: Analyzing and Detecting Fake Removal Information Advertisement Sites. Lecture Notes in Computer Science, 2020, , 171-191.	1.3	3
13	Detecting and Understanding Online Advertising Fraud in the Wild. IEICE Transactions on Information and Systems, 2020, E103.D, 1512-1523.	0.7	5
14	To Get Lost is to Learn the Way: Automatically Collecting Multi-step Social Engineering Attacks on the Web. , 2020, , .		7
15	Exploration into Gray Area: Efficient Labeling for Malicious Domain Name Detection. , 2019, , .		4
16	Precise and Robust Detection of Advertising Fraud. , 2019, , .		3
17	Efficient Dynamic Malware Analysis for Collecting HTTP Requests using Deep Learning. IEICE Transactions on Information and Systems, 2019, E102.D, 725-736.	0.7	2
18	ShamFinder. , 2019, , .		19

#	Article	IF	Citations
19	Detecting Dynamic IP Addresses and Cloud Blocks Using the Sequential Characteristics of PTR Records. Journal of Information Processing, 2019, 27, 525-535.	0.4	3
20	Cross-Vendor Knowledge Transfer for Managed Security Services with Triplet Network. , 2019, , .		2
21	Detection Method of Homograph Internationalized Domain Names with OCR. Journal of Information Processing, 2019, 27, 536-544.	0.4	3
22	DomainChroma: Building actionable threat intelligence from malicious domain names. Computers and Security, 2018, 77, 138-161.	6.0	12
23	DomainProfiler: toward accurate and early discovery of domain names abused in future. International Journal of Information Security, 2018, 17, 661-680.	3.4	7
24	Event De-Noising Convolutional Neural Network for Detecting Malicious URL Sequences from Proxy Logs. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2018, E101.A, 2149-2161.	0.3	2
25	Don't throw me away. , 2018, , .		8
26	DomainChroma: Providing Optimal Countermeasures against Malicious Domain Names. , 2017, , .		0
27	Malicious URL sequence detection using event de-noising convolutional neural network. , 2017, , .		22
28	Efficient Dynamic Malware Analysis Based on Network Behavior Using Deep Learning. , 2016, , .		46
29	DomainProfiler: Discovering Domain Names Abused in Future. , 2016, , .		27
30	Detection of vulnerability scanning using features of collective accesses based on information collected from multiple honeypots. , 2016, , .		1
31	BotProfiler: Detecting Malware-Infected Hosts by Profiling Variability of Malicious Infrastructure. IEICE Transactions on Communications, 2016, E99.B, 1012-1023.	0.7	2
32	Crawler classification using ant-based clustering scheme. , 2015, , .		0
33	BotProfiler: Profiling Variability of Substrings in HTTP Requests to Detect Malware-Infected Hosts. , 2015, , .		9
34	Analyzing Spatial Structure of IP Addresses for Detecting Malicious Websites. Journal of Information Processing, 2013, 21, 539-550.	0.4	2
35	Detecting Android Malware by Analyzing Manifest Files. Proceedings of the Asia-Pacific Advanced Network, 2013, 36, 23.	0.3	58
36	Detecting Malicious Websites by Learning IP Address Features. , 2012, , .		36