Elias Bou-Harb

List of Publications by Year
in descending order

86	1,984	361413	330143
papers	citations	20 h-index	37 g-index

86	86	86	1476
all docs	docs citations	times ranked	citing authors

#	Article	IF	Citations
1	Inferring and Investigating IoT-Generated Scanning Campaigns Targeting a Large Network Telescope. IEEE Transactions on Dependable and Secure Computing, 2022, 19, 402-418.	5.4	20
2	On Ransomware Family Attribution Using Pre-Attack Paranoia Activities. IEEE Transactions on Network and Service Management, 2022, 19, 19-36.	4.9	16
3	A survey on security applications of P4 programmable switches and a STRIDE-based vulnerability assessment. Computer Networks, 2022, 207, 108800.	5.1	21
4	A live digital forensics approach for quantum mechanical computers. Forensic Science International: Digital Investigation, 2022, 40, 301341.	1.7	0
5	An attentive interpretable approach for identifying and quantifying malware-infected internet-scale IoT bots behind a NAT. , 2022, , .		1
6	EVOLIoT. , 2022, , .		5
7	HoneyComb: A Darknet-Centric Proactive Deception Technique For Curating IoT Malware Forensic Artifacts. , 2022, , .		3
8	An Exhaustive Survey on P4 Programmable Data Plane Switches: Taxonomy, Applications, Challenges, and Future Trends. IEEE Access, 2021, 9, 87094-87155.	4.2	68
9	Vec2UAge: Enhancing underage age estimation performance through facial embeddings. Forensic Science International: Digital Investigation, 2021, 36, 301119.	1.7	0
10	A Multidimensional Network Forensics Investigation of a State-Sanctioned Internet Outage. , 2021, , .		1
11	Sanitizing the IoT Cyber Security Posture: An Operational CTI Feed Backed up by Internet Measurements. , 2021, , .		5
12	A Multi-Dimensional Deep Learning Framework for IoT Malware Classification and Family Attribution. IEEE Transactions on Network and Service Management, 2021, 18, 1165-1177.	4.9	40
13	A behavioral-based forensic investigation approach for analyzing attacks on water plants using GANs. Forensic Science International: Digital Investigation, 2021, 37, 301198.	1.7	6
14	A Strings-Based Similarity Analysis Approach for Characterizing IoT Malware and Inferring Their Underlying Relationships. IEEE Networking Letters, 2021, 3, 161-165.	1.9	16
15	Revisiting IoT Fingerprinting behind a NAT. , 2021, , .		1
16	Fingerprinting IoT Devices with Machine Learning. , 2021, , 1-4.		0
17	Dynamic Router's Buffer Sizing using Passive Measurements and P4 Programmable Switches. , 2021, , .		3
18	A Big Data-Enabled Consolidated Framework for Energy Efficient Software Defined Data Centers in IoT Setups. IEEE Transactions on Industrial Informatics, 2020, 16, 2687-2697.	11.3	75

#	Article	IF	Citations
19	On data-driven curation, learning, and analysis for inferring evolving internet-of-Things (IoT) botnets in the wild. Computers and Security, 2020, 91, 101707.	6.0	42
20	An emulation-based evaluation of TCP BBRv2 Alpha for wired broadband. Computer Communications, 2020, 161, 212-224.	5.1	25
21	Leveraging SONiC Functionalities in Disaggregated Network Switches. , 2020, , .		1
22	Stochastic Modeling, Analysis and Investigation of IoT-Generated Internet Scanning Activities. IEEE Networking Letters, 2020, 2, 159-163.	1.9	8
23	Offloading Media Traffic to Programmable Data Plane Switches. , 2020, , .		9
24	A Blockchain-based Method for Decentralizing the ACME Protocol to Enhance Trust in PKI. , 2020, , .		7
25	Exploiting Ransomware Paranoia For Execution Prevention. , 2020, , .		8
26	Towards a Unified In-Network DDoS Detection and Mitigation Strategy. , 2020, , .		20
27	Cyber Threat Intelligence for the Internet of Things. , 2020, , .		7
28	A Scalable Platform for Enabling the Forensic Investigation of Exploited IoT Devices and Their Generated Unsolicited Activities. Forensic Science International: Digital Investigation, 2020, 32, 300922.	1.7	2
29	A Collaborative Security Framework for Software-Defined Wireless Sensor Networks. IEEE Transactions on Information Forensics and Security, 2020, 15, 2602-2615.	6.9	57
30	Predictive Cyber Situational Awareness and Personalized Blacklisting. ACM Transactions on Management Information Systems, 2020, 11, 1-16.	2.8	20
31	A survey of methods supporting cyber situational awareness in the context of smart cities. Journal of Big Data, 2020, 7, .	11.0	19
32	Taxonomy of IoT Vulnerabilities. , 2020, , 7-58.		2
33	Internet-scale Insecurity of Consumer Internet of Things. ACM Transactions on Management Information Systems, 2020, 11, 1-24.	2.8	14
34	Towards Inferring IoT Maliciousness. , 2020, , 59-76.		0
35	Theoretic derivations of scan detection operating on darknet traffic. Computer Communications, 2019, 147, 111-121.	5.1	9
36	A Review of Recent Advances and Security Challenges in Emerging E-Enabled Aircraft Systems. IEEE Access, 2019, 7, 63164-63180.	4.2	11

#	Article	IF	Citations
37	Decentralized Distribution of PCP Mappings Over Blockchain for End-to-End Secure Direct Communications. IEEE Access, 2019, 7, 110159-110173.	4.2	10
38	Data-driven Curation, Learning and Analysis for Inferring Evolving IoT Botnets in the Wild. , 2019, , .		14
39	Enabling TCP Pacing using Programmable Data Plane Switches. , 2019, , .		17
40	Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations. IEEE Communications Surveys and Tutorials, 2019, 21, 2702-2733.	39.4	468
41	Comprehending the IoT cyber threat landscape: A data dimensionality reduction technique to infer and characterize Internet-scale IoT probing campaigns. Digital Investigation, 2019, 28, S40-S49.	3.2	41
42	A Comprehensive Tutorial on Science DMZ. IEEE Communications Surveys and Tutorials, 2019, 21, 2041-2078.	39.4	20
43	Survey of Attack Projection, Prediction, and Forecasting in Cyber Security. IEEE Communications Surveys and Tutorials, 2019, 21, 640-660.	39.4	172
44	Big Data Sanitization and Cyber Situational Awareness: A Network Telescope Perspective. IEEE Transactions on Big Data, 2019, 5, 439-453.	6.1	8
45	CSC-Detector: A System to Infer Large-Scale Probing Campaigns. IEEE Transactions on Dependable and Secure Computing, 2018, 15, 364-377.	5.4	7
46	On Inferring and Characterizing Large-Scale Probing and DDoS Campaigns. , 2018, , 461-474.		1
47	Data-Driven Intelligence for Characterizing Internet-Scale IoT Exploitations. , 2018, , .		2
48	On the Collaborative Inference of DDoS: An Information-theoretic Distributed Approach. , 2018, , .		0
49	Passive inference of attacks on CPS communication protocols. Journal of Information Security and Applications, 2018, 43, 110-122.	2.5	3
50	Implications of Theoretic Derivations on Empirical Passive Measurements for Effective Cyber Threat Intelligence Generation. , 2018, , .		5
51	Assessing Internet-wide Cyber Situational Awareness of Critical Sectors. , 2018, , .		12
52	Internet of Malicious Things: Correlating Active and Passive Measurements for Inferring and Characterizing Internet-Scale Unsolicited IoT Devices. IEEE Communications Magazine, 2018, 56, 170-177.	6.1	32
53	On Secrecy Bounds of MIMO Wiretap Channels with ZF detectors. , 2018, , .		3
54	Inferring, Characterizing, and Investigating Internet-Scale Malicious IoT Device Activities: A Network Telescope Perspective. , 2018, , .		17

#	Article	IF	Citations
55	Cyber Meets Control: A Novel Federated Approach for Resilient CPS Leveraging Real Cyber Threat Intelligence. , 2017, 55, 198-204.		31
56	Behavioral Service Graphs: A formal data-driven approach for prompt investigation of enterprise and internet-wide infections. Digital Investigation, 2017, 20, S47-S55.	3.2	7
57	On correlating network traffic for cyber threat intelligence: A Bloom filter approach. , 2017, , .		2
58	On the Sequential Pattern and Rule Mining in the Analysis of Cyber Security Alerts. , 2017, , .		11
59	Big Data Behavioral Analytics Meet Graph Theory: On Effective Botnet Takedowns. IEEE Network, 2017, 31, 18-26.	6.9	25
60	On the impact of empirical attack models targeting marine transportation. , 2017, , .		14
61	A first empirical look on internet-scale exploitations of IoT devices. , 2017, , .		8
62	Internet-scale Probing of CPS: Inference, Characterization and Orchestration Analysis. , 2017, , .		53
63	Towards a Big Data Architecture for Facilitating Cyber Threat Intelligence. , 2016, , .		8
64	A Brief Survey of Security Approaches for Cyber-Physical Systems. , 2016, , .		23
65	Behavioral Service Graphs: A Big Data Approach for Prompt Investigation of Internet-Wide Infections. , 2016, , .		0
66	Towards the Leveraging of Data Deduplication to Break the Disk Acquisition Speed Limit. , 2016, , .		1
67	Passive inference of attacks on SCADA communication protocols. , 2016, , .		6
68	A probabilistic model to preprocess darknet data for cyber threat intelligence generation. , 2016, , .		5
69	A novel cyber security capability: Inferring Internet-scale infections by correlating malware and probing activities. Computer Networks, 2016, 94, 327-343.	5.1	26
70	On the inference and prediction of DDoS campaigns. Wireless Communications and Mobile Computing, 2015, 15, 1066-1078.	1.2	17
71	A Time Series Approach for Inferring Orchestrated Probing Campaigns by Analyzing Darknet Traffic. , 2015, , .		12
72	Inferring distributed reflection denial of service attacks from darknet. Computer Communications, 2015, 62, 59-71.	5.1	36

#	Article	IF	Citations
73	Behavioral analytics for inferring large-scale orchestrated probing events. , 2014, , .		16
74	Fingerprinting Internet DNS Amplification DDoS Activities. , 2014, , .		29
75	Inferring internet-scale infections by correlating malware and probing activities. , 2014, , .		7
76	Multidimensional investigation of source port 0 probing. Digital Investigation, 2014, 11, S114-S123.	3.2	23
77	Cyber Scanning: A Comprehensive Survey. IEEE Communications Surveys and Tutorials, 2014, 16, 1496-1519.	39.4	127
78	On fingerprinting probing activities. Computers and Security, 2014, 43, 35-48.	6.0	31
79	A secure, efficient, and costâ€effective distributed architecture for spam mitigation on LTE 4G mobile networks. Security and Communication Networks, 2013, 6, 1478-1489.	1.5	4
80	A Statistical Approach for Fingerprinting Probing Activities. , 2013, , .		18
81	A systematic approach for detecting and clustering distributed cyber scanning. Computer Networks, 2013, 57, 3826-3839.	5.1	20
82	Towards a Forecasting Model for Distributed Denial of Service Activities. , 2013, , .		27
83	On detecting and clustering distributed cyber scanning. , 2013, , .		2
84	A first look on the effects and mitigation of VoIP SPIT flooding in 4G mobile networks. , 2012, , .		0
85	Investigating the dark cyberspace: Profiling, threat-based analysis and correlation. , 2012, , .		20
86	Training and Teaching Students and IT Professionals on High-throughput Networking and Cybersecurity Using a Private Cloud. , 0, , .		1