Future Generation Computer Systems
Volume 104, March 2020, Pages 159-173

EsPADA: Enhanced Payload Analyzer for malware Detection robust against Adversarial threats (Article)

Maestre Vidal, J.[a,c], Sotelo Monge, M.A.[b], Monterrubio, S.M.M.[c]

Save all to author list

[a]Indra, Digital Labs, Av. de Bruselas, 35, 28108 Alcobendas, Madrid, Spain
[b] Universidad de Lima, Avenida Javier Prado Este 4600, Lima, Peru
[c]Department of Software Engineering and Artificial Intelligence (DISIA), School of Computer Science, Complutense University of Madrid, Calle Profesor José García Santesmases 9, Ciudad Universitaria, Madrid, 28040, Spain

Abstract

View references (53)

The emergent communication technologies landscape has consolidated the anomaly-based intrusion detection paradigm as one of the most prominent solutions able to discover unprecedented malicious traits. It relied on building models of the normal/legitimate activities registered at the protected systems, from them analyzing the incoming observations looking for significant discordances that may reveal misbehaviors. But in the last years, the adversarial machine learning paradigm introduced never-seen-before evasion procedures able to jeopardize the traditional anomaly-based methods, thus entailing one of the major emerging challenges in the cybersecurity landscape. With the aim on contributing to their adaptation against adversarial threats, this paper presents EsPADA (Enhanced Payload Analyzer for malware Detection robust against Adversarial threats), a novel approach built on the grounds of the PAYL sensor family. At the SPARTA Training stage, both normal and adversarial models are constructed according to features extracted by N-gram, which are stored within Counting Bloom Filters (CBF). In this way it is possible to take advantage of both binary-based and spectral-based traffic modeling procedures for malware detection. At Detection stage, the payloads to be analyzed are collected from the protected environment and compared with the usage models previously built at Training. This leads to calculate different scores that allow to discriminate their nature (normal or suspicious) and to assess the labeling coherency, the latest studied for estimating the likelihood of the payload disguising mimicry attacks. The effectiveness of EsPADA was demonstrated on the public datasets DARPA'99 and UCM 2011 by achieving promising preliminarily results. © 2019 Elsevier B.V.

Author keywords

Adversarial machine learning | Anomaly recognition | Communication networks | Intrusion detection | Malware

Indexed keywords

Engineering controlled terms: Intrusion detection | Machine learning | Telecommunication networks

Engineering uncontrolled terms: Anomaly recognition | Anomaly-based intrusion detection | Building model | Communication technologies | Counting bloom filters | Cyber security | Detection stage | Malware detection

Engineering main heading: Malware

Funding details

Funding sponsor	Funding number	Acronym

Funding sponsor	Funding number	Acronym
Universidad Complutense de Madrid		UCM
Horizon 2020 Framework Programme See opportunities by H2020	830892,H2020-SU-ICT-03-2018/830892	H2020
North Atlantic Treaty Organization		NATO
Secretaría de Estado de Investigacion, Desarrollo e Innovacion		I+D+i
Fondo Nacional de Desarrollo Científico, Tecnológico y de Innovación Tecnológica		FONDECYT
Horizon 2020		
Consejo Nacional de Innovación, Ciencia y Tecnología		CONICYT
Fondo Nacional de Desarrollo Científico y Tecnológico		FONDECYT
Seventh Framework Programme		FP7
State of New Jersey Economic Development Authority		EDA
Horizon 2020 Framework Programme See opportunities by H2020		H2020

Funding text #1

This work is funded by the European Commission Horizon 2020 Programme under grant agreement number 830892, as part of the project H2020-SU-ICT-03-2018/830892 SPARTA: Special projects for advanced research and technology in Europe Thanks to the Secretariat of Education, Technology and Innovation of Mexico City (SECTEI) for their support with the third author's postdoctoral fellowship during his studies at the Complutense University of Madrid.

Funding text #2

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper. Jorge Maestre Vidal (https://jmaestrevidal.com) is PhD. in Computer Science, and Senior Specialist in cyber defense at Indra, being part of its Digital Labs division. He is the Technical Coordinator of the Indra's solutions for Cyber Situational Awareness acquisition for supporting military decision-making, leading the related technical activites conducted on National and International innovation programmes, like the EDA projects Cyber Defence Situation Awareness Package - Rapid Research Prototype (CySAP-RRP) (EDA 16.CAT.OP.078.) or Generation of Data Sets for Validation of Cyber Defence Tools (Cat. B FC B-1508-GP). He is former member of the Department of Software Engineering and Artificial Intelligence (DISIA) of the Faculty of Computer Science and Engineering at the Complutense University of Madrid (UCM), Spain. ... View all

ISSN: 0167739X
CODEN: FGCSE
Source Type: Journal
Original language: English

DOI: 10.1016/j.future.2019.10.022
Document Type: Article
Publisher: Elsevier B.V.

References (53)

View in search results format >

All | CSV export | Print | E-mail | Save to PDF | Create bibliography

1 Garcia-Teodoro, P., Diaz-Verdejo, J.E., Tapiador, J.E., Salazar-Hernandez, R.

Automatic generation of HTTP intrusion signatures by selective identification of anomalies

(2015) *Computers and Security*, 55, pp. 159-174. Cited 8 times.
doi: 10.1016/j.cose.2015.09.007

View at Publisher

2 Karami, A.
An anomaly-based intrusion detection system in presence of benign outliers with visualization capabilities

(2018) *Expert Systems with Applications*, 108, pp. 36-60. Cited 8 times.
doi: 10.1016/j.eswa.2018.04.038

View at Publisher

3 Wang, K., Stolfo, S.J.
Anomalous payload-based network intrusion detection

(2004) *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 3224, pp. 203-222. Cited 302 times.

View at Publisher

4 Wang, K., Cretu, G., Stolfo, S.J.
Anomalous payload-based worm detection and signature generation

(2006) *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 3858 LNCS, pp. 227-246. Cited 77 times.
ISBN: 3540317783; 978-354031778-4

View at Publisher

5 Bolzoni, D.
(2006) , pp. 144-156.
S. Etalle, P. Hartel, E. Zambon, POSEIDON: a 2-tier anomaly-based network intrusion detection system, in: Proceedings of the 4th IEEE International Workshop on Information Assurance, IWIA, London, United Kingdom

6 Thorat, S., Khandelwal, A., Bruhadeshwar, B., Kishore, K.
Anomalous packet detection using partitioned payload
(2009) *J. Inf. Assur. Secur.*, 3 (3), pp. 195-220. Cited 6 times.

7 Wang, K., Parekh, J.J., Stolfo, S.J.
Anagram: A content anomaly detector resistant to mimicry attack

(2006) *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 4219 LNCS, pp. 226-248. Cited 138 times.
http://springerlink.com/content/0302-9743/copyright/2005/
ISBN: 354039723X; 978-354039723-6

View at Publisher

8 Perdisci, R., Ariu, D., Fogla, P., Giacinto, G., Lee, W.
McPAD: A multiple classifier system for accurate payload-based anomaly detection

(2009) *Computer Networks*, 53 (6), pp. 864-881. Cited 148 times.
doi: 10.1016/j.comnet.2008.11.011

View at Publisher

9 Jamdagni, A., Tan, Z., He, X., Nanda, P., Liu, R.P.
RePIDS: A multi tier Real-time Payload-based Intrusion Detection System

(2013) *Computer Networks*, 57 (3), pp. 811-824. Cited 38 times.
doi: 10.1016/j.comnet.2012.10.002

View at Publisher

10 García Villalba, L.J., Sandoval Orozco, A.L., Maestre Vidal, J.
Advanced Payload Analyzer Preprocessor

(2017) *Future Generation Computer Systems*, 76, pp. 474-485. Cited 5 times.
doi: 10.1016/j.future.2016.10.032

View at Publisher

11 Hadziosmanovik, D., Simionato, L., Bolzoni, D., Zambon, E.
(2012) , pp. 59-81.
S. Etalle, N-gram against the machine: On the feasibility of the n-gram network analysis for binary protocols, in: Proceedings of the 15th International Symposium on Recent Advances in Intrusion Detection, RAID, Amsterdam, The Netherlands

12 Viswanathan, A., Tan, K., Neuman, C.
Deconstructing the assessment of anomaly-based intrusion detectors

(2013) *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 8145 LNCS, pp. 286-306. Cited 6 times.
ISBN: 978-364241283-7
doi: 10.1007/978-3-642-41284-4_15

View at Publisher

13 Pastrana, S., Orfila, A., Tapiador, J.E., Peris-Lopez, P.
Randomized Anagram revisited

(2014) *Journal of Network and Computer Applications*, 41 (1), pp. 182-196. Cited 8 times.
http://www.elsevier.com/inca/publications/store/6/2/2/8/9/3/index.htt
doi: 10.1016/j.jnca.2013.11.006

View at Publisher

14 Maestre Vidal, J., Sandoval Orozco, A.L., García Villalba, L.J.
Alert correlation framework for malware detection by anomaly-based packet payload analysis

(2017) *Journal of Network and Computer Applications*, 97, pp. 11-22. Cited 6 times.
http://www.elsevier.com/inca/publications/store/6/2/2/8/9/3/index.htt
doi: 10.1016/j.jnca.2017.08.010

View at Publisher

15 Sidorov, G., Velasquez, F., Stamatatos, E., Gelbukh, A., Chanona-Hernández, L.
Syntactic N-grams as machine learning features for natural language processing

(2014) *Expert Systems with Applications*, 41 (3), pp. 853-860. Cited 105 times.
doi: 10.1016/j.eswa.2013.08.015

View at Publisher

16 Rottenstreich, O., Keslassy, I.
The bloom paradox: When not to use a bloom filter

(2015) *IEEE/ACM Transactions on Networking*, 23 (3), art. no. 6748924, pp. 703-716. Cited 18 times.
doi: 10.1109/TNET.2014.2306060

View at Publisher

17 Maestre Vidal, J., Lucila Sandoval Orozco, A., Javier García Villalba, L.
Online masquerade detection resistant to mimicry

(2016) *Expert Systems with Applications*, 61, pp. 162-180. Cited 6 times.
doi: 10.1016/j.eswa.2016.05.036

View at Publisher

18 Shana, J., Venkatachalam, T.
An improved method for counting frequent itemsets using bloom filter (Open Access)

(2015) *Procedia Computer Science*, 47 (C), pp. 84-91. Cited 6 times.
http://www.sciencedirect.com/science/journal/18770509
doi: 10.1016/j.procs.2015.03.186

View at Publisher

19 Hadziosmanovik, D., Simionato, L., Bolzoni, D., Zambon, E.
(2012) , pp. 59-81.
S. Etalle, N-gram against the machine: On the feasibility of the n-gram network analysis for binary protocols, in: Proceedings of the 15th International Symposium on Recent Advances in Intrusion Detection, RAID, Amsterdam, The Netherlands

20 Edgeworth, F.
On discordant observations
(1887) *Phil. Mag.*, 33 (5). Cited 39 times.

21 Chandola, V., Banerjee, A., Kumar, V.
Anomaly detection: A survey

(2009) *ACM Computing Surveys*, 41 (3), art. no. 15. Cited 3746 times.
doi: 10.1145/1541880.1541882

View at Publisher

22 Zimek, A., Campello, R., Sander, J.
Ensembles for unsupervised outlier detection: challenges and research questions
(2013) *ACM SIGKDD Explor. Newsl.*, 15 (1), pp. 11-22. Cited 98 times.

23 Barona López, L.I., Valdivieso Caraguay, Á.L., Vidal, J.M., Sotelo Monge, M.A., García Villalba, L.J.
Towards incidence management in 5G based on situational awareness (Open Access)

(2017) *Future Internet*, 9 (1), art. no. 3. Cited 6 times.
http://www.mdpi.com/1999-5903/9/1/3/pdf
doi: 10.3390/fi9010003

View at Publisher

24 Motzek, A., Möller, R.
Context- and bias-free probabilistic mission impact assessment (Open Access)

(2017) *Computers and Security*, 65, pp. 166-186. Cited 7 times.
doi: 10.1016/j.cose.2016.11.005

View at Publisher

25 Buczak, A.L., Guven, E.
A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection (Open Access)

(2016) *IEEE Communications Surveys and Tutorials*, 18 (2), art. no. 7307098, pp. 1153-1176. Cited 376 times.
http://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=9739
doi: 10.1109/COMST.2015.2494502

View at Publisher

26 Aggarwal, C.C.
Outlier analysis

(2013) *Outlier Analysis*, 9781461463962, pp. 1-446. Cited 455 times.
http://dx.doi.org/10.1007/978-1-4614-6396-2
ISBN: 978-146146396-2; 1461463955; 978-146146395-5
doi: 10.1007/978-1-4614-6396-2

View at Publisher

27 Pevný, T.
Loda: Lightweight on-line detector of anomalies (Open Access)

(2016) *Machine Learning*, 102 (2), pp. 275-304. Cited 21 times.
doi: 10.1007/s10994-015-5521-0

View at Publisher

28 Ahmed, M., Naser Mahmood, A., Hu, J.
A survey of network anomaly detection techniques

(2016) *Journal of Network and Computer Applications*, 60, pp. 19-31. Cited 230 times.
http://www.elsevier.com/inca/publications/store/6/2/2/8/9/3/index.htt
doi: 10.1016/j.jnca.2015.11.016

View at Publisher

29 Corona, I., Giacinto, G., Roli, F.
Adversarial attacks against intrusion detection systems: Taxonomy, solutions and open issues

(2013) *Information Sciences*, 239, pp. 201-225. Cited 61 times.
doi: 10.1016/j.ins.2013.03.022

View at Publisher

30 Ditzler, G., Roveri, M., Alippi, C., Polikar, R.
Learning in Nonstationary Environments: A Survey

(2015) *IEEE Computational Intelligence Magazine*, 10 (4), art. no. 7296710, pp. 12-25. Cited 180 times.
http://www.ieee.org/products/onlinepubs/news/0705_02.html#2
doi: 10.1109/MCI.2015.2471196

View at Publisher

31 Zimmermann, A.
The data problem in data mining
(2014) *ACM SIGKDD Explor. Newsl.*, 16 (2), pp. 38-45. Cited 6 times.

32 Polakis, I., Diamantaris, M., Petsas, T., Maggi, F., Ioannidis, S.
Powerslave: Analyzing the energy consumption of mobile antivirus software

(2015) *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 9148, pp. 165-184. Cited 4 times.
http://springerlink.com/content/0302-9743/copyright/2005/
ISBN: 978-331920549-6
doi: 10.1007/978-3-319-20550-2_9

View at Publisher

33 Biggio, B., Roli, F.
Wild patterns: Ten years after the rise of adversarial machine learning

(2018) *Pattern Recognition*, 84, pp. 317-331. Cited 39 times.
www.elsevier.com/inca/publications/store/3/2/8/
doi: 10.1016/j.patcog.2018.07.023

View at Publisher

34 Fogla, P., Sharif, M., Perdisci, R., Kolesnikov, O., Lee, W.
Polymorphic blending attacks
(2006) , pp. 241-256. Cited 113 times.
Proceedings of the 15th USENIX Security Symposium, Vancouver, BC, Canada

35 Ariu, D., Tronci, R., Giacinto, G.
HMMPayl: An intrusion detection system based on Hidden Markov Models

(2011) *Computers and Security*, 30 (4), pp. 221-241. Cited 71 times.
doi: 10.1016/j.cose.2010.12.004

View at Publisher

36 Swarnkar, M., Hubballi, N.
OCPAD: One class Naive Bayes classifier for payload based anomaly detection

(2016) *Expert Systems with Applications*, 64, pp. 330-339. Cited 15 times.
doi: 10.1016/j.eswa.2016.07.036

View at Publisher

37 Jin, X., Cui, B., Li, D., Cheng, Z., Yin, C.
An improved payload-based anomaly detector for web applications

(2018) *Journal of Network and Computer Applications*, 106, pp. 111-116. Cited 3 times.
http://www.elsevier.com/inca/publications/store/6/2/2/8/9/3/index.htt
doi: 10.1016/j.jnca.2018.01.002

View at Publisher

38 Baychev, Y., Bilge, L.
Spearphishing malware: Do we really know the unknown?

(2018) *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 10885 LNCS, pp. 46-66. Cited 2 times.
https://www.springer.com/series/558
ISBN: 978-331993410-5
doi: 10.1007/978-3-319-93411-2_3

View at Publisher

39 Gencosman, B.C., Ozmutlu, H.C., Ozmutlu, S.
Character n-gram application for automatic new topic identification

(2014) *Information Processing and Management*, 50 (6), pp. 821-856. Cited 11 times.
doi: 10.1016/j.ipm.2014.06.005

View at Publisher

40 Raff, E., Zak, R., Cox, R., Sylvester, J., Yacci, P., Ward, R., Tracy, A., (...), Nicholas, C.
An investigation of byte n-gram features for malware classification

(2018) *Journal of Computer Virology and Hacking Techniques*, 14 (1). Cited 17 times.
http://www.springer.com/computer/journal/11416
doi: 10.1007/s11416-016-0283-1

View at Publisher

41 Geravand, S., Ahmadi, M.
Bloom filter applications in network security: A state-of-the-art survey

(2013) *Computer Networks*, 57 (18), pp. 4047-4064. Cited 67 times.
http://www.journals.elsevier.com/computer-networks/
doi: 10.1016/j.comnet.2013.09.003

View at Publisher

42 Rieck, K., Laskov, P.
Detecting unknown network attacks using language models

(2006) *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 4064 LNCS, pp. 74-90. Cited 38 times.
http://springerlink.com/content/0302-9743/copyright/2005/
ISBN: 354036014X; 978-354036014-8

View at Publisher

43 Jonathon, T., Somesh, J., Miller, B.
Automated discovery of mimicry attacks
(2006) , pp. 41-60.
Proceedings of the 9th International Symposium on Recent Advances in Intrusion Detection, RAID, Hamburg, Germany

44 Tapiador, J., Clark, J.
Information-theoretic detection of masquerade mimicry attacks
(2010)
Proceedings of the 4th International Conference on Network and System Security, Melbourne, VIC, Australia.

45 Green, R., Staffell, I., Vasilakos, N.
Divide and Conquer? k-means clustering of demand data allows rapid and accurate simulations of the British electricity system

(2014) *IEEE Transactions on Engineering Management*, 61 (2), art. no. 6729088, pp. 251-260. Cited 45 times.
doi: 10.1109/TEM.2013.2284386

View at Publisher

46 Satopää, V., Albrecht, J., Irwin, D., Raghavan, B.
Finding a "kneedle" in a haystack: Detecting knee points in system behavior

(2011) *Proceedings - International Conference on Distributed Computing Systems*, art. no. 5961514, pp. 166-171. Cited 72 times.
ISBN: 978-076954386-4
doi: 10.1109/ICDCSW.2011.20

View at Publisher

47 Grosse, K., Papernot, N., Manoharan, P., Backes, M., McDaniel, P.
Adversarial examples for malware detection

(2017) *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 10493 LNCS, pp. 62-79. Cited 38 times.
http://springerlink.com/content/0302-9743/copyright/2005/
ISBN: 978-331966398-2
doi: 10.1007/978-3-319-66399-9_4

View at Publisher

48 Papernot, N., McDaniel, P., Wu, X., Jha, S., Swami, A.
Distillation as a defense to adversarial perturbations against deep neural networks
(2016) , pp. 62-79. Cited 35 times.
Proceedings of the 2016 IEEE Symposium on Security and Privacy, SP, San Jose, CA, USA

49 Ciftcioglu, E., Hardy, R., Chan, K., Scott, L., Oliveira, D., Verma, G.
Chaff allocation and performance for network traffic obfuscation
(2018)
Proceedings of the 38th International Conference on Distributed Computing Systems, ICDCS, Vienna, Austria.

50 Lippmann, R., Haines, J.W., Fried, D.J., Korba, J., Das, K.
1999 DARPA off-line intrusion detection evaluation

(2000) *Computer Networks*, 34 (4), pp. 579-595. Cited 493 times.
doi: 10.1016/S1389-1286(00)00139-0

View at Publisher

51 Mchugh, J.
Testing Intrusion Detection Systems: A Critique of the 1998 and 1999 DARPA Intrusion Detection System Evaluations as Performed by Lincoln Laboratory

(2000) *ACM Transactions on Information and System Security*, 3 (4), pp. 262-294. Cited 671 times.
doi: 10.1145/382912.382923

View at Publisher

52 Cohen, E., Kaplan, H.
What you can do with coordinated samples

(2013) *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 8096 LNCS, pp. 452-467. Cited 7 times.
ISBN: 978-364240327-9
doi: 10.1007/978-3-642-40328-6_32

View at Publisher

53 Bantis, L.E., Nakas, C.T., Reiser, B.
Construction of confidence regions in the ROC space after the estimation of the optimal Youden index-based cut-off point

(2014) *Biometrics*, 70 (1), pp. 212-223. Cited 39 times.
doi: 10.1111/biom.12107

View at Publisher

Maestre Vidal, J.; Indra, Digital Labs, Av. de Bruselas, 35, 28108 Alcobendas, Madrid, Spain;
email:jmaestre@ucm.es