[a1]

SonicWall

Sonicwall cyber threat report

<https://www.sonicwall.com/medialibrary/en/white-paper/2023-cyber-threat-report.pdf> (2023)

[a2]

Gopinath M., Sibi Chakkaravarthy Sethuraman Ph.D., A comprehensive survey on deep learning based malware detection techniques

[a3] Hyrum S Anderson and Phil Roth. 2018. Ember: an open dataset for training static PE malware machine learning models. arXiv preprint arXiv:1804.04637 (2018).

[a4] George E Dahl, Jack W Stokes, Li Deng, and Dong Yu. 2013. Large-scale malware classification using random projections and neural networks. In 2013 IEEE Inter national Conference on Acoustics, Speech and Signal Processing. IEEE, 3422–3426.

[a5] Edward Raff, Jon Barker, Jared Sylvester, Robert Brandon, Bryan Catanzaro, and Charles K Nicholas. 2018. Malware detection by eating a whole exe. In Workshops at the Thirty-Second AAAI Conference on Artificial Intelligence.

[a6] Konrad Rieck, Philipp Trinius, Carsten Willems, and Thorsten Holz. 2011. Auto matic analysis of malware behavior using machine learning. Journal of Computer Security 19, 4 (2011), 639–668.

[a7] Joshua Saxe and Konstantin Berlin. 2015. Deep neural network based malware de tection using two dimensional binary program features. In 2015 10th International Conference on Malicious and Unwanted Software (MALWARE). IEEE, 11–20.

[a8]J.X. Geng, J.F. Wang, Z.Y. Fang, Y.J. Zhou, D. Wu, W.H. Ge

A survey of strategy-driven evasion methods for PE malware: transformation, concealment, and attack

Comput. Secur., 137 (2024), Article 103595, [10.1016/j.cose.2023.103595](https://doi.org/10.1016/j.cose.2023.103595)

[a9]

HyrumSAnderson,AnantKharkar,BobbyFilar,DavidEvans,andPhilRoth.2018. Learning to evade static PE machine learning malware models via reinforcement learning. arXiv preprint arXiv:1801.08917 (2018).

[a10]

Luca Demetrio, B. Biggio, Giovanni Lagorio, F. Roli, and A. Armando. 2020. Functionality-preserving Black-box Optimization of Adversarial Windows Mal ware. arXiv: Cryptography and Security (2020).

[a11]

Erwin Quiring, Alwin Maier, and Konrad Rieck. 2019. Misleading authorship attribution of source code using adversarial learning. In 28th {USENIX} Security Symposium ({USENIX} Security 19). 479–496.

[a12]

Dazhi Zhan, Wei Bai, Xin Liu, Yue Hu, Lei Zhang, Shize Guo, and Zhisong Pan. 2023. PSP-Mal: Evading malware detection via prioritized experience-based reinforcement learning with Shapley prior. In *Proceedings of the 39th Annual Computer Security Applications Conference*. 580–593.

[a13]H.S. Anderson, A. Kharkar, B. Filar, P. Roth

Evading Machine Learning Malware Detection

Black Hat (2017)

[a14] H.S. Anderson, A. Kharkar, B. Filar, D. Evans, P. Roth

Learning to evade static pe machine learning malware models via reinforcement learning

ArXiv preprint

[arXiv:1801.08917](http://arxiv.org/abs/1801.08917) (2018)

[a15]W. Song, X. Li, S. Afroz, D. Garg, D. Kuznetsov, H. Yin

Mab-malware: a reinforcement learning framework for blackbox generation of adversarial malware

Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security (2022), pp. 990-1003

[a16] Z. Fang, J. Wang, B. Li, S. Wu, Y. Zhou, H. Huang

Evading anti-malware engines with deep reinforcement learning

IEEE Access, 7 (2019), pp. 48867-48879

[a17]R. Labaca-Castro, S. Franz, G.D. Rodosek

Aimed-rl: exploring adversarial malware examples with reinforcement learning

Machine Learning and Knowledge Discovery in Databases. Applied Data Science Track: European Conference, ECML, Proceedings, Part IV 21, PKDD 2021, Bilbao, Spain, September 13–17, 2021, Springer (2021), pp. 37-52

[a18]D. Gibert, M. Fredrikson, C. Mateu, J. Planes, Q. Le

Enhancing the insertion of nop instructions to obfuscate malware via deep reinforcement learning

Comput. Secur., 113 (2022), Article 102543

[a19]I.J. Goodfellow, J. Shlens, C. Szegedy

Explaining and harnessing adversarial examples

3rd International Conference on Learning Representations, ICLR 2015 - Conference Track Proceedings (2015)

[a20]N. Carlini, D. Wagner

Towards evaluating the robustness of neural networks

2017 IEEE Symposium on Security and Privacy (SP), IEEE (2017), pp. 39-57

[a21] S.M. Moosavi-Dezfooli, A. Fawzi, P. Frossard

Deepfool: a simple and accurate method to fool deep neural networks

Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (2016), pp. 2574-2582

[a22] B. Kolosnjaji, A. Demontis, B. Biggio, D. Maiorca, G. Giacinto, C. Eckert, F. Roli

Adversarial malware binaries: evading deep learning for malware detection in executables

2018 26th European Signal Processing Conference (EUSIPCO), IEEE (2018), pp. 533-

[a23] A. Al-Dujaili, A. Huang, E. Hemberg, U.M. O'Reilly

Adversarial deep learning for robust detection of binary encoded malware

2018 IEEE Security and Privacy Workshops (SPW), IEEE (2018), pp. 76-

[a24] F. Kreuk, A. Barak, S. Aviv-Reuven, M. Baruch, B. Pinkas, J. Keshet

Deceiving end-to-end deep learning malware detectors using adversarial examples

ArXiv preprint

[a25] O. Suciu, S.E. Coull, J. Johns

Exploring adversarial examples in malware detection

2019 IEEE Security and Privacy Workshops (SPW) (2019), pp. 8-14

[a26] X. Liu, J. Zhang, Y. Lin, H. Li

Atmpa: attacking machine learning-based malware visualization detection methods via adversarial examples

Proceedings of the International Symposium on Quality of Service (2019), pp. 1-10

[a27] D. Park, H. Khan, B. Yener

Generation & evaluation of adversarial examples for malware obfuscation

2019 18th IEEE International Conference on Machine Learning and Applications (ICMLA), IEEE (2019), pp. 1283-1290

[a28]

Statista

Global market share held by operating systems for desktop PCs, from january 2013 to february 2024

(2024)

<https://www.statista.com/statistics/218089/global-market-share-of-windows-7/>. [Online; Accessed 2024]

**a[29]**

AV-TEST

Statistics

(2023)

<https://portal.av-atlas.org/malware/statistics>. [Online; Accessed 2023]

[a30]G. A Rummery and M. Niranjan, Online Q-learning using connection systems.

Technical Report, Cambridge University, 1994.

[a31]R. S. Sutton and A. G. Barto, Reinforcement learning: An introduction(2nd Edition).MIT Press, 2018

[a32]H. Van Seijen, H. Van Hassekt, S. Whiteson, and M. Wiering, “A theoretical and empirical analysis of Expected Sarsa,” in IEEE Symposium on Adaptive Dynamic Programming and Reinforcement Learning, 2009, pp. 177-184

[a33]M. Ganger, E. Duryea, and W. Hu,“Double Sarsa and double expected Sarsa with shallow and deep learning,” Journal of Data Analysis and Information Processing, vol.4, no.4,2016, pp. 159-176

[a34]Yokoyama A., Ishii K., Tanabe R., Papa Y., Yoshioka K., Matsumoto T., Kasama T., Inoue D., Brengel M., Backes M., *et al.*

Sandprint: Fingerprinting malware sandboxes to provide intelligence for sandbox evasion

International Symposium on Research in Attacks, Intrusions, and Defenses, Springer (2016), pp. 165-187

[a35]Rudd E., Rozsa A., Gunther M., Boult T.

A survey of stealth malware: Attacks, mitigation measures, and steps toward autonomous open world solutions

IEEE Commun. Surv. Tutor., 19 (2) (2017), pp. 1145-1172

[a36]Bulazel A., Yener B.

A survey on automated dynamic malware analysis evasion and counter-evasion: PC, mobile, and web

Proceedings of the 1st Reversing and Offensive-Oriented Trends Symposium, ACM, ACM, New York, NY, USA (2017), p. 2

[a37]Apostolopoulos T., Katos V., Choo K.-K.R., Patsakis C.

Resurrecting anti-virtualization and anti-debugging: Unhooking your hooks

Future Gener. Comput. Syst., 116 (2021), pp. 393-405

[a38]"Parasitic malware: The resurgence of an old threat", Network Security, vol. 3, pp. 15-18, 2008.

[a39]2012 IEEE Symposium on Security and Privacy

Smashing the Gadgets: Hindering Return-Oriented Programming Using In-Place Code Randomization

Vasilis Pappas, Michalis Polychronakis, and Angelos D. Keromytis

Columbia University

[a40] Jithin Pavithran, Milan Patnaik, and Chester Rebeiro. 2019. D-TIME: Distributed Threadless Independent Malware Execution for Runtime Obfuscation. In 13th USENIX Workshop on Offensive Technologies (WOOT 19). USENIX Association, Santa Clara, CA. https://www.usenix.org/conference/woot19/presentation/ pavithran

[a41] Kyriakos K. Ispoglou and Mathias Payer. 2016. malWASH: Washing Malware to Evade Dynamic Analysis. In 10th USENIX Workshop on Offensive Technolo gies (WOOT 16). USENIX Association, Austin, TX. https://www.usenix.org/ conference/woot16/workshop-program/presentation/ispoglou

[a42] J. Xie, S. Li, X. chun Yun, Y. Zhang, P. Chang

Hstf-model: an http-based Trojan detection model via the hierarchical spatio-temporal features of traffics

Comput. Secur., 96 (2020), Article 101923