DETEKSI DAN KLASIFIKASI *MALWARE* PADA CITRA *GRAYSCALE* DENGAN MENGGUNAKAN *DEEP LEARNING*

Diajukan Sebagai Syarat Untuk Menyelesaikan
Pendidikan Program Strata-1 Pada
Jurusan Teknik Informatika

Oleh :

Daniel Sandwi Victory
NIM : 09021181823024

Jurusan Teknik Informatika

FAKULTAS ILMU KOMPUTER UNIVERSITAS SRIWIJAYA

2023

LEMBAR PENGESAHAN SKRIPSI

Deteksi dan Klasifikasi Malware pada Citra Grayscale dengan menggunakan Deep Learning

Oleh :

Daniel Sandwi Victory
NIM : 09021181823024

Indralaya, 2 Agustus 2023

Pembimbing I	Pembimbing II
Julian Supardi, S.Pd., M.T., Ph.D.	Osvari Arsalan,S.Kom., M.T.
NIP. 197207102010121001	NIP. 198806282018031001

Mengetahui,
Ketua Jurusan Teknik Informatika

Alvi Syahrini Utami, M.Kom.
NIP. 197812222006042003

TANDA LULUS UJIAN KOMPREHENSIF SKRIPSI

Pada hari Rabu tanggal 24 Juli 2023 telah dilaksanakan ujian komprehensif skripsi oleh Jurusan Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya.

Nama	:	Daniel Sandwi Victory
NIM	:	09021181823024
Judul	:	Deteksi dan Klasifikasi Malware pada Citra Grayscale dengan menggunakan Deep Learning

dan dinyatakan **LULUS.**

1. Ketua Penguji

Kanda Januar Miraswan, M.T. ....
NIP. 199001092019031012

2. Penguji

Dr. M. Fachrurrozi, M.T. .....
NIP. 198005222008121002

3. Pembimbing I

Julian Supardi, S.Pd., M.T., Ph.D. .....
NIP. 197207102010121001

4. Pembimbing II

Osvari Arsalan,S.Kom., M.T. .....
NIP. 198806282018031001

Mengetahui,
Ketua Jurusan Teknik Informatika

Alvi Syahrini Utami, M.Kom.
NIP. 197812222006042003

HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini :

Nama	: Daniel Sandwi Victory
Nim	: 09021181823024
Prodi	: Teknik Informatika
Judul Skirpsi	: Deteksi dan Klasifikasi Malware pada Citra Grayscale dengan Deep Learning

Hasil pengecekan Sofware *iThenticate/Turnitin* : 17%

Menyatakan bahwa Laporan Proyek saya merupakan hasil karya sendiri dan bukan hasil penjiplakan/plagiat. Apabila ditemukan unsur penjiplakan/plagiat dalam Laporan Proyek ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya sesuai dengan ketentuan yang berlaku.

Demikian pernyataan ini saya buat dengan sebenar-benarnya dan tidak ada paksaan oleh siapa pun.

Indralaya, 2 Agustus 2023

Daniel Sandwi Victory
NIM. 09021181823024

MOTTO DAN PERSEMBAHAN

It's okay to be weak, but it's not okay to stay weak

Kupersembahkan karya tulis ini kepada:

- Orang Tua dan Keluargaku
- Teman-teman seperjuangan
- Dosen Pembimbing
- Fakultas Ilmu Komputer Universitas Sriwijaya

Detection and Classification of Malware in Grayscale Images using Deep Learning

By:

Daniel Sandwi Victory (09021181823024)

ABSTRACT

This research focuses on the utilization of Deep Learning techniques for malware detection and classification. By representing malware samples as grayscale images, a Deep Learning model based on Convolutional Neural Networks (CNN) is developed. The model is trained using a dataset containing grayscale malware samples. Experimental results demonstrate a high level of accuracy of the Deep Learning model in detecting and classifying malware. This research contributes to the advancement of computer security systems by effectively addressing the challenges posed by malware threats using the Deep Learning approach. The research results show that the evaluation of the testing results on the trained model architecture yielded an average Accuracy of 0.96, Precision of 0.97, Recall of 0.97, and F1-Score of 0.96 using 20% of the dataset, consisting of 474 malware images.

Keywords: malware detection, malware classification, Deep Learning, grayscale images, Convolutional neural networks (CNNs)

Indralaya, 2 August 2023

Supervisor I	Supervisor II
Julian Supardi, S.Pd., M.T., Ph.D.	Osvari Arsalan,S.Kom., M.T.
NIP. 197207102010121001	NIP. 198806282018031001

Approved,
Head of Informatics department

Alvi Syahrini Utami, M.Kom.
NIP. 197812222006042003

Deteksi dan Klasifikasi Malware pada Citra Grayscale dengan menggunakan Deep Learning

Oleh:

Daniel Sandwi Victory (09021181823024)

ABSTRAK

Penelitian ini berfokus pada penggunaan teknik *Deep Learning* untuk deteksi dan klasifikasi *malware*. Dengan mewakili sampel *malware* sebagai gambar *grayscale*, sebuah model *Deep Learning* berbasis *Convolutional neural networks* (CNN) dikembangkan. Model ini dilatih menggunakan *dataset* yang berisi sampel *malware* dalam bentuk *grayscale*. Hasil eksperimen menunjukkan tingkat akurasi yang tinggi dari model *Deep Learning* dalam mendeteksi dan mengklasifikasikan *malware*. Penelitian ini memberikan kontribusi dalam pengembangan sistem keamanan komputer dengan efektif menghadapi tantangan yang ditimbulkan oleh ancaman malware menggunakan pendekatan *Deep Learning*. Hasil penelitian menunjukkan bahwa evaluasi hasil pengujian pada arsitektur model yang telah dilatih menghasilkan rata-rata *Accuracy* sebesar 0.96, *Precision* sebesar 0.97, *Recall* sebesar 0.97, dan *F1-Score* 0.96 dengan menggunakan 20% dari *dataset*, yang terdiri dari 474 gambar malware.

Kata Kunci: deteksi *malware,* klasifikasi *malware, Deep Learning,* gambar *grayscale, Convolutional neural networks* (CNN).

Indralaya, 2 Agustus 2023

Pembimbing I	Pembimbing II
Julian Supardi, S.Pd., M.T., Ph.D.	Osvari Arsalan,S.Kom., M.T.
NIP. 197207102010121001	NIP. 198806282018031001

Mengetahui,
Ketua Jurusan Teknik Informatika

Alvi Syahrini Utami, M.Kom.
NIP. 197812222006042003

KATA PENGANTAR

Puji dan syukur saya panjatkan kepada Tuhan Yang Maha Esa atas rahmat-Nya yang melimpah sehingga saya dapat menyelesaikan Tugas Akhir dalam menyelesaikan studi untuk mendapatkan gelar sarjana pada jurusan Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya dengan judul skripsi "Deteksi dan Klasifikasi *Malware* Pada Citra *Grayscale* Dengan Menggunakan *Deep Learning*".

Dalam kesempatan ini penulis mengucapkan terima kasih kepada pihak-pihak yang telah banyak membantu dalam pelaksanaan dan penyusunan skripsi ini diantaranya :

1. Orang tua saya yang selalu memberikan dukungan, doa, dan semangat hingga motivasi yang tiada henti.
2. Bapak Julian Supardi, S.Pd., M.T., Ph.D. selaku Pembimbing 1 yang telah meluangkan waktu, tenaga, dan pemikirannya dalam membimbing penulis sehingga dapat menyelesaikan skripsi ini
3. Bapak Osvari Arsalan, S.Kom., M.T. selaku Pembimbing 2 yang telah membantu, membimbing dalam pembuatan skripsi dan perangkat lunak sehingga penulis dapat menyelesaikan skripsi ini.
4. Bapak Dr. Abdiansah, S.Kom., M.CS. selaku dosen pembimbing akademik yang telah membimbing, mengarahkan dan memberikan motivasi penulis dalam proses perkuliahan.
5. Ibu Alvi Syahrini Utami, S.Si, M.Kom. selaku Ketua Jurusan Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya.
6. Teman-teman perkuliahan di Universitas Sriwijaya yang telah menemani penulis selama perkuliahan dan memberikan masa perkuliahan yang menyenangkan.

7. Seluruh dosen Program Studi Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya.
8. Bapak dan Ibu dosen Fakultas Ilmu Komputer Universitas Sriwijaya yang telah memberikan penulis ilmu dan mengajar penulis berbagai macam mata kuliah yang bermanfaat selama masa perkuliahan.
9. Teman-teman saya Roni Starko Firdaus, Genta Agsal Valendri, Muhammad Tiansyah Pratama, Ananda Meilizar Dwi Putra, Agung Sukrisna Jaya, Renaldi Budi Setiawan, Gustino Mayindra Putra dan lain-lainnya yang sudah membantu dan menemani saya selama ini.

Dalam penyusunan laporan ini, penulis menyadari masih banyak kekurangan baik dari segi susunan serta cara penulisan laporan ini, karenanya saran dan kritik yang sifatnya membangun demi kesempurnaan laporan ini sangat penulis harapkan. Akhirnya, semoga laporan ini bisa bermanfaat bagi para pembaca pada umumnya dan juga bermanfaat bagi penyusun pada khususnya.

Indralaya, 2 Agustus 2023

Penulis,

Daniel Sandwi Victory

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Pendahuluan

Bab ini memberikan penjelasan mengenai latar belakang penelitian, perumusan masalah, tujuan dan manfaat penelitian, batasan masalah atau cakupan penelitian, serta tata cara penulisan.

1.2 Latar Belakang

Seiring berkembangnya jaman, teknologi mengalami peningkatan yang maju. Semuanya mengadaptasi digital dari cara kerja manual. Teknologi memiliki kelebihan dan kekurangan, yang dimana disatu sisi mempermudah hidup dan disisi lain mengundang tindak kejahatan seperti serangan *cyber*, hilangnya data, dan kebocoran data pribadi yang dimana dapat disalahgunakan oleh pihak yang tidak bertanggung-jawab. Oleh karena itu keamanan perangkat sangat penting di dunia *cyber* saat ini. Penggunaan internet semakin hari semakin meningkat. Salah satu kelemahan dari penggunaan internet adalah banyak sistem komputer yang rentan terhadap serangan *malware*. (Heena, 2021).

Malware merupakan program jahat yang dapat menyebabkan kerusakan pada file dan sistem informasi. (Mustafa Majid et al., 2021). Konsekuensi dari keberadaan *malware* ini dapat mencakup kerusakan pada sistem komputer dan juga memungkinkan terjadinya pencurian data. Salah satu penyebab umum terjadinya infeksi *malware* adalah melalui unduhan perangkat lunak ilegal yang mungkin mengandung *malware* yang disisipkan di dalamnya. Terdapat beberapa

jenis *Malware* seperti *virus*, *worm, trojan horse*, *spyware*, serta *software-software* lain yang berbahaya. Banyak penyerang *cyber* yang telah menggunakan teknik yang berbeda untuk menyebarkan *malware* untuk alasan moneter dan lainnya. Penyerang memiliki keuntungan ekonomi dalam melakukan serangan tersebut. Karena ada lebih banyak jenis *malware*, metode deteksi *malware* menjadi sangat diperlukan untuk keamanan data.

Serangan *malware* merupakan ancaman yang sangat serius bagi dunia maya saat ini. Meskipun para peneliti dan perusahaan *anti-malware* berupaya keras untuk memerangi serangan *malware*, jumlah *malware* terus meningkat secara signifikan, seperti yang tercatat dalam laporan terbaru tentang ancaman keamanan siber oleh Symantec. Para penjahat siber melihat adanya keuntungan yang tinggi dalam penggunaan *malware*, sehingga mereka meluncurkan berbagai kampanye melalui *ransomware*, *Trojan* perbankan, *virus*, dan metode lainnya. Selain itu, banyak serangan siber, seperti serangan penolakan layanan terdistribusi, umumnya menggunakan *malware* sebagai sarana utama untuk melancarkan serangan. Menurut laporan terbaru dari Accenture, biaya ekonomi akibat serangan *malware* yang berhasil sangatlah mengkhawatirkan, dengan perkiraan rata-rata kerugian sebesar $2,6 juta per serangan. Tingginya tingkat serangan *malware* ini telah mendorong banyak penelitian guna mengurangi dan mencegah serangan-serangan tersebut. (Darem et al., 2021)

Baru-baru ini, teknik *Deep Learning* telah terbukti efektif dalam beberapa tugas klasifikasi. Oleh karena itu, tugas ini menerapkan penggunaan *Deep Learning* untuk mengatasi masalah ini. Menurut Munawa & Putri, 2020, *Deep*

Learning merupakan bagian dari kategori keluarga algoritma *Machine learning* yang lebih luas, yang beroperasi dengan menggunakan prinsip dasar pembelajaran. Baik pembelajaran yang diawasi maupun yang tidak diawasi dapat digunakan dalam metode *Deep Learning*. *Deep Learning* melibatkan penggunaan jaringan saraf tiruan dengan banyak lapisan. Setiap lapisan dalam *Deep Learning* terdiri dari sejumlah *neuron* yang dilengkapi dengan fungsi aktivasi untuk menghasilkan keluaran yang bersifat *non-linear*. Metodologi ini didasarkan pada inspirasi dari struktur neuron otak manusia. Pada *Deep Learning*, model yang dikomputerisasi akan melakukan serangkaian tugas seperti klasifikasi atau analisis pola yang khusus, berdasarkan pengetahuan yang diperoleh dari data yang telah dipelajari sebelumnya. Oleh karena itu, sebuah model harus menjalani proses pelatihan terlebih dahulu dengan menggunakan kumpulan data yang telah diberi label.

Untuk mendeteksi apakah citra target berbahaya, digunakan metode *Deep Learning* untuk mempelajari fitur diskriminatif dari jejak eksekusi. Dalam penelitian yang berjudul *MDCHD: A novel malware detection method in cloud using hardware trace and Deep Learning*, peneliti menggunakan *MDCHD* dengan mekanisme *Intel Processor Trace* (IPT) untuk mengumpulkan informasi aliran kontrol *run-time* dari program target yang akan diteliti. Kemudian mengubah informasi aliran kontrol menjadi gambar berwarna. Penulis mengimplementasikan metode *Deep Learning* berbasis *Convolutional neural network* (CNN) untuk mengidentifikasi *malware* dari gambar-gambar. Evaluasi menunjukkan bahwa pendekatan peneliti dapat mencapai akurasi deteksi yang dapat diterima dengan

biaya kinerja minimal. CNN dikenal memiliki performa sangat baik dalam menangkap fitur level tinggi secara otomatis, CNN telah banyak digunakan dalam banyak pengenalan pola tugas seperti klasifikasi gambar dan segmentasi. CNN juga dapat digunakan sebagai pengklasifikasian final. (Tian et al., 2021)

Sehubungan dengan itu, berdasarkan latar belakang dan penjelasan yang telah disampaikan, penelitian ini akan menerapkan *Deep Learning* dalam bentuk *Convolutional Neural Network* untuk melakukan deteksi dan klasifikasi *malware*.

1.3 Rumusan Masalah

Berdasarkan informasi yang telah dijelaskan sebelumnya, peneliti akan mengidentifikasi fokus masalah yang akan dibahas dalam penelitian ini, yaitu bagaimana menerapkan *Deep Learning* dalam melakukan deteksi dan klasifikasi terhadap *malware* dan juga bagaimana merancang arsitektur model *Convolutional Neural Network* yang optimal untuk deteksi dan klasifikasi *malware*, yang dimana rancangan model akan dilakukan analisis terhadap *dataset* yang berisi kumpulan file berupa gambar *malware* untuk menghasilkan tingkat akurasi pengujian (*Test Accuracy*) yang tinggi.

1.4 Tujuan Penelitian

Dari paparan diatas yang dijelaskan sebelumnya, terdapat beberapa tujuan yang ingin dicapai oleh peneliti melalui tugas akhir ini, antara lain :

1. Melakukan pengembangan perangkat lunak yang menerapkan metode *Convolutional neural network* dalam Deteksi dan Klasifikasi *Malware*.
2. Membangun rancangan arsitektur model *Convolutional Neural Network* yang dapat melakukan klasifikasi *malware*.

3. Mengetahui hasil kinerja dari rancangan arsitektur model *Convolutional Neural Network* yang dibangun.
4. Mengevaluasi hasil pengujian dan kinerja arsitektur model *Convolutional Neural Network* dalam melakukan klasifikasi *malware*.

1.5 Manfaat Penelitian

Manfaat penelitian ini adalah sebagai berikut:

1. Dapat membantu pengguna sistem dalam mendeteksi *malware* dengan menggunakan penerapan *Deep Learning*.
2. Meningkatkan keamanan data pengguna
3. Hasil penelitian juga dapat dipakai sebagai rujukan untuk penelitian-penelitian deteksi dan klasifikasi *malware* dengan *Deep Learning* selanjutnya.

1.6 Batasan Penelitian

Berikut adalah batasan masalah yang diberlakukan dalam penelitian ini :

1. Metode yang dipakai pada tugas ini berupa CNN.
2. Penelitian ini menggunakan *dataset* berupa file *malware* yang sudah diubah menjadi gambar *grayscale* dengan format PNG.
3. Penelitian ini hanya melakukan pendeteksian dan pengklasifikasian jenis *malware* pada *dataset* yang dipakai.
4. Rancangan aplikasi ini hanya dapat mendeteksi dokumen yang sudah diubah terlebih dahulu menjadi gambar *Grayscale* dari 25 jenis *malware* yang dipakai dalam penelitian.

1.7 Sistematika Penulisan

Sistematika penulisan tugas akhir ini mengikuti standar penulisan yang telah ditetapkan oleh Fakultas Ilmu Komputer Universitas Sriwijaya. Berikut adalah struktur yang akan diikuti dalam penulisan tugas akhir ini :

BAB I. PENDAHULUAN

Bab ini akan menjelaskan mengenai latar belakang, perumusan masalah, tujuan dan manfaat penelitian, batasan masalah atau cakupannya, serta pengaturan penulisan.

BAB II. KAJIAN LITERATUR

Bab ini akan menguraikan konsep dasar dan teori yang terkait dengan topik penelitian yang sedang dilakukan, serta aspek-aspek yang relevan dalam menganalisis permasalahan. Selain itu, bab ini juga akan memberikan tinjauan analisis terhadap penelitian-penelitian sebelumnya yang relevan, serta menyusun sintesis dari hasil tinjauan tersebut.

BAB III. METODOLOGI PENELITIAN

Dalam bab ini, akan dibahas tentang tahap-tahap yang akan dilakukan dalam penelitian. Setiap tahapan penelitian akan dijelaskan secara terperinci sesuai dengan kerangka kerja yang telah ditetapkan. Selanjutnya, akan dibahas pula perancangan manajemen proyek yang akan diterapkan dalam pelaksanaan penelitian.

BAB IV. PENGEMBANGAN PERANGKAT LUNAK

Bab pengembangan perangkat lunak akan mencakup topik-topik seperti arsitektur, diagram, implementasi *Convolutional neural network* (CNN) dalam deteksi dan klasifikasi *malware*, serta hasil pengujian perangkat lunak.

BAB V. HASIL DAN ANALISIS PENELITIAN

Bab hasil dan analisis akan menggambarkan secara detail hasil penelitian yang telah dijelaskan pada bab sebelumnya dalam bentuk tabel dan grafik. Informasi ini akan menjadi dasar untuk mencapai kesimpulan yang akan diambil dalam penelitian ini.

BAB VI. KESIMPULAN DAN SARAN

Bab ini merupakan bagian kesimpulan dari seluruh uraian yang ada pada bab-bab sebelumnya. Selain itu, bab ini juga akan menyajikan saran-saran yang diharapkan dapat bermanfaat dalam penerapan *Deep Learning* di masa yang akan datang.

1.8 Kesimpulan

Pada pendahuluan ini, telah dijelaskan secara umum mengenai penelitian yang akan dilakukan, meliputi latar belakang, rumusan masalah, tujuan dan manfaat penelitian, batasan masalah serta sistematika penulisan.

DAFTAR PUSTAKA

Abdelsalam, M., Krishnan, R., Huang, Y., & Sandhu, R. (2018). Malware Detection in Cloud Infrastructures Using Convolutional Neural Networks. *IEEE International Conference on Cloud Computing, CLOUD*, *2018-July*, 162–169. https://doi.org/10.1109/CLOUD.2018.00028

Abdulrahman, A., & Varol, S. (2020). A Review of Image Segmentation Using MATLAB Environment. *8th International Symposium on Digital Forensics and Security, ISDFS 2020*, 8–12. https://doi.org/10.1109/ISDFS49300.2020.9116191

Alawneh, H., Umphress, D., & Skjellum, A. (2019). *Android Malware Detection Using Neural Networks & Process Control Block Information*. *August*. https://www.researchgate.net/publication/337010589

Albelwi, S., & Mahmood, A. (2017). A framework for designing the architectures of deep Convolutional Neural Networks. *Entropy*, *19*(6). https://doi.org/10.3390/e19060242

Alzaylaee, M. K., Yerima, S. Y., & Sezer, S. (2020). DL-Droid: *Deep Learning* based android malware detection using real devices. *Computers and Security*, *89*, 101663. https://doi.org/10.1016/j.cose.2019.101663

Bejiga, M. B., Zeggada, A., Nouffidj, A., & Melgani, F. (2017). A convolutional neural network approach for assisting avalanche search and rescue operations with UAV imagery. *Remote Sensing*, *9*(2). https://doi.org/10.3390/rs9020100

Berman, D. S., Buczak, A. L., Chavis, J. S., & Corbett, C. L. (2019). A survey of

Deep Learning methods for cyber security. *Information (Switzerland)*, *10*(4). https://doi.org/10.3390/info10040122

Darem, A., Abawajy, J., Makkar, A., Alhashmi, A., & Alanazi, S. (2021). Visualization and deep-learning-based malware variant detection using OpCode-level features. *Future Generation Computer Systems*, *125*, 314–323. https://doi.org/10.1016/j.future.2021.06.032

Deng, L., & Yu, D. (2013). *Deep Learning*: Methods and applications. *Foundations and Trends in Signal Processing*, *7*(3–4), 197–387. https://doi.org/10.1561/2000000039

Gibert, D., Mateu, C., Planes, J., & Vicens, R. (2019). Using convolutional neural networks for classification of malware represented as images. *Journal of Computer Virology and Hacking Techniques*, *15*(1), 15–28. https://doi.org/10.1007/s11416-018-0323-0

Hadiprakoso, R. B., Qomariasih, N., & Yasa, R. N. (2021). Identifikasi Malware Android Menggunakan Pendekatan Analisis Hibrid Dengan *Deep Learning*. *Jurnal Teknologi Informasi Universitas Lambung Mangkurat (JTIULM)*, *6*(2), 77–84. https://doi.org/10.20527/jtiulm.v6i2.82

Heena. (2021). *Advances In Malware Detection- An Overview*. http://arxiv.org/abs/2104.01835

Hijazi, S., Kumar, R., & Rowen, C. (2015). What Is a CNN? Using Convolutional Neural Networks for Image Recognition. *Cadence Whitepaper*, *6*(11), 1–12.

Hu, F., Xia, G. S., Hu, J., & Zhang, L. (2015). Transferring deep convolutional neural networks for the scene classification of high-resolution remote sensing

imagery. *Remote Sensing*, *7*(11), 14680–14707. https://doi.org/10.3390/rs71114680

Kumar, A. K., Haseeb, M. A., Kumar, G. N., & Goud, E. A. (2022). *IMAGE BASED CLASSIFICATION OF MALWARE USING DEEP LEARNING*. *06*, 2480–2485.

Maggiori, E., Tarabalka, Y., Charpiat, G., & Alliez, P. (2017). Convolutional Neural Networks for Large-Scale Remote-Sensing Image Classification. *IEEE Transactions on Geoscience and Remote Sensing*, *55*(2), 645–657. https://doi.org/10.1109/TGRS.2016.2612821

Martin, B. (2018). *D Eep C Onvolutional M Alware C Lassifiers C an*. *2016*, 2016–2019.

Munawa, Z., & Putri, N. I. (2020). Keamanan IoT Dengan *Deep Learning* dan Teknologi Big Data. *Tematik : Jurnal Teknologi Informasi Komunikasi (e-Journal)*, *7*(2), 161–185. https://jurnal.plb.ac.id/index.php/tematik/article/view/479

Mustafa Majid, A.-A., Alshaibi, A. J., Kostyuchenko, E., & Shelupanov, A. (2021). A review of artificial intelligence based malware detection using *Deep Learning*. *Materials Today: Proceedings*, *xxxx*. https://doi.org/10.1016/j.matpr.2021.07.012

Nahmias, D., Cohen, A., Nissim, N., & Elovici, Y. (2019). TrustSign: Trusted Malware Signature Generation in Private Clouds Using Deep Feature Transfer Learning. *Proceedings of the International Joint Conference on Neural Networks*, *2019-July*(July), 1–8.

https://doi.org/10.1109/IJCNN.2019.8851841

Nahmias, D., Cohen, A., Nissim, N., & Elovici, Y. (2020). Deep feature transfer learning for trusted and automated malware signature generation in private cloud environments. *Neural Networks*, *124*, 243–257. https://doi.org/10.1016/j.neunet.2020.01.003

Nataraj, L., Karthikeyan, S., Jacob, G., & Manjunath, B. S. (2011). Malware images: Visualization and automatic classification. *ACM International Conference Proceeding Series*, *July 2014*. https://doi.org/10.1145/2016904.2016908

Or-Meir, O., Nissim, N., Elovici, Y., & Rokach, L. (2019). Dynamic malware analysis in the modern era—A state of the art survey. *ACM Computing Surveys*, *52*(5). https://doi.org/10.1145/3329786

Raff, E., Barker, J., Sylvester, J., Brandon, R., Catanzaro, B., & Nicholas, C. (2017). *Malware Detection by Eating a Whole EXE*. http://arxiv.org/abs/1710.09435

Ren, Z., Wu, H., Ning, Q., Hussain, I., & Chen, B. (2020). End-to-end malware detection for android IoT devices using *Deep Learning*. *Ad Hoc Networks*, *101*, 102098. https://doi.org/10.1016/j.adhoc.2020.102098

Rezende, E., Ruppert, G., Carvalho, T., Theophilo, A., Ramos, F., & de Geus, P. (2018). Malicious Software Classification Using VGG16 Deep Neural Network's Bottleneck Features. *Advances in Intelligent Systems and Computing*, *738*, 51–59. https://doi.org/10.1007/978-3-319-77028-4_9

Simonyan, K., & Zisserman, A. (2015). Very deep convolutional networks for

large-scale image recognition. *3rd International Conference on Learning Representations, ICLR 2015 - Conference Track Proceedings*, 1–14.

Tian, D., Ying, Q., Jia, X., Ma, R., Hu, C., & Liu, W. (2021). MDCHD: A novel malware detection method in cloud using hardware trace and *Deep Learning*. *Computer Networks*, *198*(April), 108394. https://doi.org/10.1016/j.comnet.2021.108394

D Eep L Earning for, 50 Jcit 50 (2020).

Zhi, T., Duan, L. Y., Wang, Y., & Huang, T. (2016). Two-stage pooling of deep convolutional features for image retrieval. *Proceedings - International Conference on Image Processing, ICIP*, *2016-Augus*, 2465–2469. https://doi.org/10.1109/ICIP.2016.7532802