ISSN: 1803-3814 (Printed), 2571-3701 (Online)
https://doi.org/10.13164/mendel.2019.2.027

A SURVEY ON ARTIFICIAL INTELLIGENCE IN MALWARE AS NEXT–GENERATION THREATS

Cong Truong Thanh[1,2,✉] **and Ivan Zelinka**[1]

[1]Department of Computer Science, VSB-Technical University of Ostrava, Czech Republic
[2]University of Finance - Marketing, Ho Chi Minh, Viet Nam
cong.thanh.truong.st@vsb.cz[✉], ivan.zelinka@vsb.cz

Abstract

Recent developments in Artificial intelligence (AI) have a vast transformative potential for both cybersecurity defenders and cybercriminals. Anti-malware solutions adopt intelligent techniques to detect and prevent threats to the digital space. In contrast, cybercriminals are aware of the new prospects too and will probably try to use it in their activities. This survey aims at providing an overview on the way artificial intelligence can be used to power a malicious program that is: intelligent evasion techniques, autonomous malware, AI against itself, and applying bio-inspired computation and swarm intelligence.

Keywords: *Artificial intelligence, machine learning, malware, computer virus, security, swarm intelligence.*

Received: 27 October 2019
Accepted: 05 December 2019
Published: 21 December 2019

1 Introduction

For recent years, AI is becoming an omnipresent trend. At this time, when using an online search engine, we can get over 4 billion results, which illustrates the interest of experts and the public. Interest in AI has been high for the past few years, reaching a peak in 2018. This hype is due to significant advances in the field of AI and their extensive applications in the real world.

Malware is malicious software that infiltrates or damage a computer system without consent and without informing the system owner. Researchers used this term to express a variety of forms of software or program code, such as computer virus, worm, trojan horse, retrovirus, botnet [43]. Its impact on digital society is enormous, so a considerable amount of research has been done to find effective measures to prevent this pandemic. Due to the impact of malware, the community has developed technologies to counter against it. Unfortunately, there are cases where new malware spreads over the Internet, making defense solutions useless. Thus, to keep pace with malware evolution, advanced techniques like Machine Learning (ML) and Deep Learning (DL) need to be used [9]. In particular, anti-malware solutions can use various intelligent techniques, such as artificial neural networks to recognize new and unknown malware codes. Generally speaking, the evolution of malware and anti-malware technologies is an ongoing tug-of-war with no end. The evolution of malware entails the development of anti-malware systems. Hence, it is important to predict, model, and confirm by experimenting with possible anti-malware software improvements to ready for new emergence threats [48].

Up to the present time, researchers published various literature discussing the dynamics and spreading of malware. The most significant trend focuses on the dynamics of malware (typically based on mathematical models) as well as the study of how malware behaves in real-world networks such as computer networks, social networks, and others. The authors in [36] study the computer virus infection by adapting the epidemiologically compartmental models. They have drawn a mathematical model and identified potential edges where contagion could occur. In the meantime, the authors in [50] proposed a heterogeneous propagation model and its optimal control problem, in which they studied the combined impact of countermeasure and network topology on virus diffusion and optimal dynamic countermeasure. Alongside that, Singh et al. [40] discussed a moderate epidemiological model, which based on the fractional epidemiological model to describe computer viruses with an arbitrary order derivative having a non-singular kernel.

The other approaches that studies malware behavior is in [26],[37],[39]. In [26], the authors combined the Susceptible Infected and the Susceptible Infected Recovered model then applied this model to the Barabasi–Albert network to determine how the infection rates affect virus propagation. In [37], Parsaei et al. combined Lyapunov functions with the Volterra-Lyapunov matrix properties to apply for a computer virus propagation model. The researchers in [39] proposed a computer virus propagation model based on the kill signals, called SEIR-KS. In this model, the authors applied the Routh-Hurwitz criterion and Lyapunov functional approach.

In another aspect of malware research, Pan and Fung [35] discussed how AI could be used in malware to enhance its effectiveness. Noreen et al. [34], Meng et al. [30] propose the evolvable malware framework using the evolutionary computation techniques to evolve computer and Android malware, respectively. Meanwhile, the authors in [6] suggested exploiting an Evolutionary Algorithm (EA) to auto-generate malware. Other papers by Kudo et al. [23],[24] presented a model of the botnets that applying machine learning techniques to predict vulnerabilities autonomously and to evolve itself. In a later study [4], scientists investigate a range of possible malicious misuses of AI (which focuses on ML) in cybersecurity, physical and political.

The aim of this article is to study the possibilities that AI could incorporate with malware to enhance its effectiveness, thereby providing the background knowledge to counter against malware in the future. Furthermore, this article will discuss some of the directions that need further study to prepare for the AI-powered malware era.

The rest of this paper proceeds as follows. Section 2 introduces a brief overview of AI and malware. Section 3 presents how AI could be applied to avoid detection. The capability of autonomously malicious software was discussed in section 4. Section 5 presents the trendy of using AI against itself. In section 6, we discuss the direction of combining bio-inspired computation and swarm intelligence in malware. Then we outline some proof of concepts in section 7. Section 8 discusses about future challenges and directions. Finally, section 9 concludes the paper.

2 Overview of the Use of AI in Malware

In 1983, Fred Cohen demonstrated a program that capability infected a computer, replicated, and spread to other computers which lead to the born of the term "computer virus" [8]. Ever since then, many advances techniques have been included in malware development such as encryption, oligomorphism, polymorphism, metamorphism, obfuscation [38], armoring (armored viruses) [16], and the dynamically executed contents (DEC) methods [33]. The goal of these techniques is to make the malware harden to understand and thus to evade anti-malware tools. Moreover, dramatic advances in ML and AI has made a significant shift in the IT industry. Consequently, cybercriminals are also aware of the benefits of AI and may try to use it to their advantage and weaponize it. To ready for the new threat, it is necessary to research how threat actors could use AI for malicious purposes.

The history of AI has been around for more than sixties years. It represents the idea of creating machines think and act like humans being. These machines can learn independently, based on data from the environment without human interference. However, today, the term AI synonymous with Machine Learning, and more recently, with Deep Learning. Machine Learning originated in the mid-1990s and its real-world applications enable computers to find patterns in increasingly large databases for classification, prediction, and other advanced tasks. Deep Learning is a strict subset of ML and has its roots in Artificial Neural Networks (ANN). While scientists progressively discovered many algorithms for DL in the period of 1980s to 2000s, DL was only noticed again for recent years with the computational power of GPUs.

It is essential to comprehend the feature of intelligent software and how to classify software as intelligent. Intelligent software is software with highly robust and adaption, can learn from experiences and react to unpredicted circumstances with a collection of different procedures. Furthermore, it must be autonomous so that it can be aware of the current state of its environment and act on its own to accomplish its goals [29]. Another approach to evaluate the intelligence of software is whether software capable mimics biological behaviors [41] like the ability of mutation, propagation, and evolution. Malware is also a software, so it is entirely possible for malware to start imitating the biological behavior to mutate, propagate, contaminate its host, evade detection, surpass countermeasures in the digital world similar to the real world. Therefore, it is logical to expect that AI-driven malware is going to be developed shortly. Fig. 1 illustrate some of the areas where the use of this technology could give the attackers an advantage.

3 Intelligent Evasion Techniques

Ever since the first computer virus (Brain) was released in the wild [43], malware development has gone a long way. As cyber defenders develop more intelligent, sophisticated, and proactive defenses, malware authors have continued to find ways to overcome them. One of the ultimate goals of malware is to hide their presence and malicious intent to avoid being detected by anti-malware solutions. Being aware of the AI's benefits, it is certain that cybercriminals will find ways to implement this technology into evasive techniques. Here are some directions that attackers can exploit:

- Dodge sandbox detection: a malware inmate as a legitimate program when analyzed by a detection tool and performs the malicious activities for only when running on an actual user's device. Cybercriminals program them to act with different behaviors base on the environment in which they are executing. Consequently, this is a useful technique for malware programs to avoid detection as long as possible. The defensive program categorizes the program as benign so that it is allowed to execute; meanwhile, it can continue to perform malicious activities. If the malware embraces with intelligent techniques, then it can autonomously decide how to react depending on the environmental factors it faces.

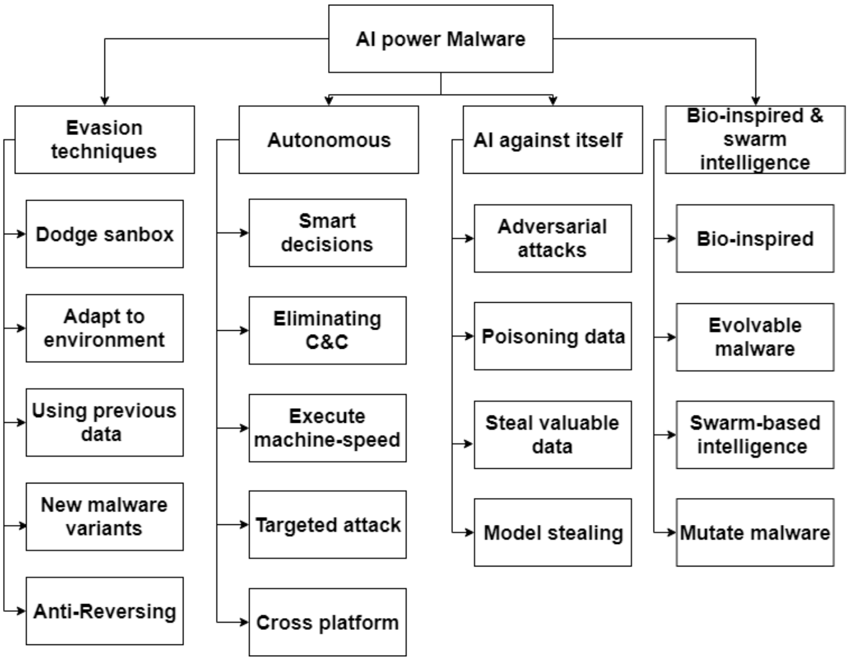

Figure 1: Taxonomy of AI techniques in malware

- Using previous data to evade detection: base on the data from preceding campaigns and the analysis of security tools, malicious actors could apply ML to develop and implement advanced obfuscation techniques to evade detection.

- Adapt to the environment: AI-powered malware will be capable adapt to the surroundings where it executes. The malware will exploit the vulnerabilities or disguised as trusted elements of the system by learning from contextual information. The longer the threat can exist in the host, the more it becomes independent, integrating into its environment, selecting tools, and taking countermeasures against security tools.

- Generate new malware variants: Attackers can use the technique of generate automated code and insert it into files and change the malware such that it evades detection algorithms. For example, the malware families Swizzor [5] were using automation to generate new variants of themselves. By using ML algorithms, this technique can be reused and enhanced to discover which new variations are less likely to be discovered and create new strains with similar characteristics.

- Anti-reversing by using backbox technique: A threatening aspect of AI-embed malware is that it could implement the “black box” technique (i.e., neural networks) to hide its malicious payload. Analysts usually use reverse engineering tools to analyze and record malware. However, neural networks are complicated to reverse, which makes attackers easier to evade security tools and experts.

4 Autonomous Malware

With the support of AI, the new generation of malware will be smarter and capable to operate autonomously. It is reasonable to expect malware in future could be aware of its environment and make calculated decisions about what to do base on the situation.

- Smarter malware: Shortly, malware could propagate base on a sequence of autonomous decisions, intelligently custom-made to the parameters of the host system. This kind of malware operates similar to branch prediction technology, which betters over time when making a prediction base on a conditional action it has seen before. We can imagine a scenario in that malware is capable of choosing lateral movement techniques to depend on its environment. Instead of exploiting the vulnerable, it can switch to brute-forcing credentials or even install a key-logger to capture credentials. Autonomous malware will then select the most successful for the target use this method to traverse.

- Eliminate command-and-control (C&C) channel: Malware could be equipped with intelligent automation and preliminary logical process to automatically navigate a compromised network, select the desired target types, and push of data to malware owner. Being able to make decisions automatically helps malware remove C&C channels in spreading and accomplishing goals. Thus, the attacks will become stealthier and more menacing.

- Execute machine-speed: AI could perform the analytical functions similar to humans – but at machine speed. Therefore, it could be used in malicious software for exploiting software vulnerabilities on a mass level, for example, an automated attack of thousands of machines per hour [4].
- Targeted and customized attacks: In another scenario, the malware authors can add the capacity to make smarter decisions into malware to maximize their profits. As a result, malware can automatically choose which payload will bring the most benefit based on the environment and the infected machine. For example, the malware can learn whether it infects the computer of a significant person in the company base on the communication of this person. On this person's computer, stealing sensitive information or locking the document for ransoming will make more profit. Conversely, if the malicious software recognizes it infected a server, then installing a crypto-miner may be a better choice. Furthermore, the malware's AI can observe and learn patterns of normal user behavior in localhost email and chat traffic, for reconnaissance. Then, it can mimic the tone and style of this user to automated composition an email and send for other employees to prompt them accessing malicious content. That would be much more effective and convincing than classic social-engineering effort.
- Cross-platform malware: Another aspect that needs to be considered is that the developing of cross-platform autonomous malware that can operate on multiplatform [28]. This type of malware carries a variety of exploit and payload tools that can operate across different environments. Based on its assessment of the target environment (including the platform information), the malware selects, assembles, and executes an attack against its target. The aim of this type of malware is that it can trigger contagion across multiple platforms so that making detection and resolution more difficult.

5 AI Against Itself

As AI is being integrated into security solutions, the attacker will attempt to hijack it by any means. Cybercriminals could tamper the dataset to deceive the AI system, tweak the data to trick anti-malware engines using ML, use the advantage of intelligent techniques to collect data, or even reverse the ML models to surpass it.

- AI in adversarial attacks: adversarial is another rising trend of AI-based threats, where malicious actors design the inputs to make models predict erroneously. There have been several studies showing how these attacks can work in diverse situations [19],[3]. These studies showed that tricking the AI's ability to recognize objects is fairly simple. The objective of an anti-malware AI is different from recognizing images, but it is fundamentally using the same kind of ML. It is provided with data to understand the elements that constitute malicious code, use algorithms and models to conduct training and refine parameters. After trained the model and verified its quality, the model is applied to pick out the potential malware. However, if AI can learn to detect potential malware, another AI should be capable learn from observing anti-malware make its decisions and use that knowledge to develop the least detectable malware. Several recent studies have demonstrated how ML systems can be evaded by other ML models [2],[46],[20],[1].
- Poisoning data: as mention above, anti-malware engines using ML learns from data. So, the ML output is poisoned if its input is poisoned, and cybercriminals are already trying to do this. The attacker could pollute the training data from which the algorithm is learning in such a way that the system misbehaves. Different domains are vulnerable to poisoning attacks, for example: network intrusion, spam filtering or malware analysis [27],[31],[7]. However, poisoning can occur in any area where training data is not verified thoroughly before being included in the model.
- Use ML for data collection: Today, enterprises use data labeling and ML to classify and capture valuable data as well as shelter their valuable data resources. In the same way, attackers can implement the same efficient technique in malware to discover the most precious business data to reduce the size of data files for stealthy exfiltration. Alongside that, with the ability to automatically analyze data mass-collected, misuse of ML will increase threats related to privacy and social manipulation.
- Model stealing: These techniques are used to thieve (for example, duplicate) models or recover training data via backbox examining [44]. In this occasion, the attacker learns how ML algorithms work by reversing techniques. From this knowledge, the malware authors know what the scanning engines are looking for and how to avoid it. For example, malicious actors could steal spam filtering models or malware prediction to be able to surpass such models.

6 Bio-Inspired Computation and Swarm Intelligence

Regarding advancing in swarm-based intelligence and technologies, it is logical to expect that, shortly swarm intelligence will be used in both attack and cyber defenses tools. Very promising algorithms (regarding malware could be derivative from) are algorithms that inspired by nature such as Genetic Algorithm [45]. Another interesting algorithm (regarding C&C worms like Botnets are) are swarm algorithms such as ant colony optimization (ACO) [13] followed by Particle Swarm Optimization (PSO) [14],[22] and Self Organizing Migration Algorithm (SOMA) [49],[47],[12].

- Bio-inspired: Concurrently to the development of malware, there are attempts to apply bio-inspired techniques into malware. For instance, in 2005, a report [15] showed that a virus named Zellome used GA as a form of brute-force approach to generate polymorphic decryptor. Although the report indicated that the implementation of GA in this virus is ineffective, the use of an evolutionary algorithm in this virus drawn some attention. Another recent study [32] present how to compromise a computer by encoding malware in a DNA sequence. Once the DNA strains were sequenced, the resulting data became a malware which corrupted the software and took control of the underlying computer. While with present technology, this is far from practical means of attack for cybercriminals, but it is a concept for the future.

- Evolvable malware: According to [21], malware will continue to evolve based on the Darwinian theory of evolution. Such malware is a real threat to the current detection methods due to a large number of functions they could apply and unable to be screened. The evolution of malware is comprising multiple steps. First, select the malware from different variants. Second, apply the evolutionary algorithm to simulate the evolution of the malware such as gene crossover (i.e., switching features of samples) and mutations (i.e., choosing feature) to produce a new generation. Finally, the newly generated malware is tested with anti-malware products. More details about the process can be found in reference [34],[30],[6]. The idea of autonomously evolved malware is frightening [21] in case applying for botnet and using AI-based techniques to select the malware samples. Fig. 2 illustrate the idea of combining the AI method to evolve malware.

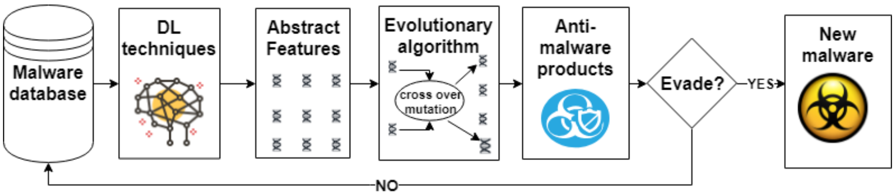

Figure 2: Apply DL for evolving malware

- Swarm-based intelligence malware: The advancement of malware shows that C&C communication has been used as in the case of Stuxnet [25] virus or Botnet malware [11]. The disadvantage of such viruses is the centralized control structure. Once the C&C center is immobile, the virus performance will be eliminated. One solution can be attained based on the framework of the swarm intelligence-based algorithms, which simulate the behavior of the biological swarm systems that usually do not have a central communication point. The communication between members in the swarm can be done variously. Every individual can have a collective memory, share knowledge as well as “learn from it.” Thus, swarm virus is the logical step in C&C kind of malware, and shortly swarm-based intelligence malware will become a new emerges threat [48].

- Mutate malware: Mutation is a concept in biology refers to a process that creates genetic variation. Inspire by this concept; attackers try to mutate the malware code to create a new one for evading the detection methods and thus making the reversing difficult. The mutation is the process of altering the malicious software without or limit changing its functionality. The mutation can be done by: alters its code structure, changes its form whenever it is executed or rewrites its code every time it is executed. The application of intelligent techniques can speed up the mutant malware process. Thus, malware authors can easily create more obfuscated malware, which capable of overcoming modern detection tools, as shown in [46],[1].

7 Related Works

Although the real AI malware has not appeared in the wild or at least not being caught yet, scientists have shown the proof of concept that computational intelligence could be used to enhance malware.

The Table 1 listing some significant proof of concepts that demonstrate the idea of adopting intelligent methods in malware

Table 1: Proof of concepts of computational intelligence methods used in malware

References	Techniques used	Main Idea
[6],[30]	Evolutionary algorithm	applying evolutionary computation to generate or evolve malware.
[17],[18]	Neural networks with supervised and unsupervised learning	encode the trojan and use neural network to decode
[1]	ML with reinforcement learning	using ML to evade ML anti-malware model
[48],[10]	Swarm Intelligence	swarm virus prototype, which mimics a swarm system behavior
[42]	Deep Learning	present a targeted and evasive AI-powered malware

8 Future Challenges and Directions

Until now, the malware that uses AI in the wild has not been caught yet, but we cannot wait until the real attack occurs to start enhancing our defenses. Therefore, the new generation of AI-integrated malware requires in-depth research to determine the feasibility of this type of attack as well as identify possible defense methods.

Future research should focus on the utilization of DL for improving malware evasion techniques. To date, scientists just studied exploiting the evolution algorithms to generate new variants of malware. However, there is a study about using a neural network as a communication layer to hide commands. This approach could be applied as a classifier to select the best evasion technique to avoid detection. The use of NN in malware methods should be investigated further.

Another aspect that necessitates being studied is the use of swarm engine in malware. Specifically, the swarm communication, which not using the canalize storage file, but the information is shared, updated, and used by all instances directly. Such malware will exhibit extremely high robustness of information preservation against swarm network damage. Swarm communication also expose the research direction to apply this idea to other malware like worms, trojans, or ransomware so that their activities can be more distributed and stealth.

Furthermore, with such above predictions, it is of crucial importance that we must have the ability to use better AI technology in cyber defense than the one attacker possess. Therefore, a lot more research needs on how to use AI in cyber defense in the AI-powered malware era.

9 Conclusion

The fight between malware and anti-malware is an endless war. Both sides try to adopt advanced techniques to increase the power to overcome the other. To ready for the era of malware strengthened by AI, it is crucial to equip the knowledge to find effective measures to prevent it. In this article, the directions that AI could be used in malware was covered. These techniques are intelligent evasion techniques, autonomous malware, AI against itself, and applying bio-inspired computation and swarm intelligence. This paper will, hopefully, offer a vision for computer system protection in the future.

Acknowledgement: The following grants are acknowledged for the financial support provided for this research: Grant of SGS No. SP2019/137, VSB Technical University of Ostrava.

References

[1] Anderson, H. S., Kharkar, A., Filar, B., Evans, D., and Roth, P. 2018. Learning to evade static pe machine learning malware models via reinforcement learning. *arXiv preprint*, arXiv:1801.08917.

[2] Anderson, H. S., Woodbridge, J., and Filar, B. 2016. Deepdga: Adversarially-tuned domain generation and detection. In *Proceedings of the 2016 ACM Workshop on Artificial Intelligence and Security*, ACM, pp. 13–21.

[3] Brown, T. B., Mane, D., Roy, A., Abadi, M., and Gilmer, J. 2017. Adversarial patch. *arXiv preprint* arXiv:1712.09665.

[4] Brundage, M. et al. 2018. The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. *arXiv preprint* arXiv:1802.07228.

[5] Calvet, J. and Bureau, P. M. 2010. Understanding swizzor's obfuscation scheme. In *REcon.*

[6] Cani, A., Gaudesi, M., Sanchez, E., Squillero, G., and Tonda, A. P. 2014. Towards automated malware creation: code generation and code integration. In *SAC*, pp. 157–160.

[7] Chen, S., et al. 2018. Automated poisoning attacks and defenses in malware detection systems: An adversarial machine learning approach. *Computers & Security* 73, 326–344.

[8] Cohen, F. 1987. Computer viruses: theory and experiments. *Computers & Security* 6, 1, 22–35.

[9] Cong, T., Zelinka, I., Plucar, J., Candik, M., and Sulc, V. 2019. Artificial intelligence and cybersecurity. To appear in *Proceedings of 4th International Conference on Artificial Intelligence and Evolutionary Computations in Engineering Systems.*

[10] Cong, T, Zelinka, I., and Senkerik, R. Neural swarm virus. To appear in *Proceedings of 7-th Joint International Conferences on Swarm, Evolutionary and Memetic Computing Conference (SEMCCO 2019) & Fuzzy And Neural Computing Conference (FANCCO 2019)*

[11] Dagon, D., Zou, C. C., and Lee, W. 2006. Modeling botnet propagation using time zones. In *NDSS*, vol. 6, pp. 2–13.

[12] Davendra, D., Zelinka, I., et al. 2016 *Self-organizing migrating algorithm.* Springer. DOI: 10.1007/978-3-319-28161-2

[13] Dorigo, M. and Birattari, M. 2010. *Ant colony optimization.* Springer.

[14] Eberhart, R. and Kennedy, J. 1995. A new optimizer using particle swarm theory. In *MHS'95 – Proceedings of the Sixth International Symposium on Micro Machine and Human Science*, IEEE, pp. 39–43.

[15] Ferrie, P. and Shannon, H. 2005. Virus analysis 2 – It's zell(d)ome the one you expect. *Virus Bulletin*, pp. 7–11.

[16] Filiol, E. 2004. Strong cryptography armoured computer viruses forbidding code analysis: The bradley virus. *Ph.D. thesis*, INRIA.

[17] Geigel, A. 2013. Neural network trojan. *Journal of Computer Security* 21, 2, 191–232.

[18] Geigel, A. 2014. Unsupervised learning trojan. *Ph.D. thesis*, Nova Southeastern University.

[19] Goodfellow, I. J., Shlens, J., and Szegedy, C. 2014. Explaining and harnessing adversarial examples. *arXiv preprint* arXiv:1412.6572.

[20] Hu, W. and Tan, Y. 2017. Generating adversarial malware examples for black-box attacks based on gan. *arXiv preprint* arXiv:1702.05983.

[21] Iliopoulos, D., Adami, C., and Szor, P. 2011. Darwin inside the machines: Malware evolution and the consequences for computer security. *arXiv preprint* arXiv:1111.2503.

[22] Kennedy, J. 2006. Swarm intelligence. In *Handbook of nature-inspired and innovative computing*, Springer, pp. 187–219.

[23] Kudo, T., Kimura, T., Inoue, Y., Aman, H., and Hirata, K. 2016. Behavior analysis of self-evolving botnets. In *2016 International Conference on Computer, Information and Telecommunication Systems (CITS)*, IEEE, pp. 1–5.

[24] Kudo, T., Kimura, T., Inoue, Y., Aman, H., and Hirata, K. 2018. Stochastic modeling of self-evolving botnets with vulnerability discovery. *Computer Communications* 124, pp. 101–110.

[25] Kushner, D. 2013. The real story of stuxnet. *IEEE Spectrum* 3, 50, pp. 48–53.

[26] Lazfi, S., Lamzabi, S., Rachadi, A., and Ez-Zahraouy, H. 2017. The impact of neighboring infection on the computer virus spread in packets on scale-free networks. *International Journal of Modern Physics B* 31, 30, 1750228. DOI: 10.1142/S0217979217502289.

[27] Li, P., Liu, Q., Zhao, W., Wang, D., and Wang, S. 2018. Bebp: an poisoning method against machine learning based idss. *arXiv preprint* arXiv:1803.03965.

[28] Lindorfer, M., Neumayr, M., Caballero, J., and Platzer, C. 2013. Poster: Cross-platform malware: write once, infect everywhere. In *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*, ACM, pp. 1425–1428.

[29] Maes, P. 1995. Intelligent software. *Scientific American* 273, 3, pp. 84–86.

[30] Meng, G., Xue, Y., Mahinthan, C., Narayanan, A., Liu, Y., Zhang, J. and Chen, T. 2016. Mystique: Evolving android malware for auditing anti-malware tools. In *Proceedings of the 11th ACM on Asia conference on computer and communications security*, ACM, pp. 365–376.

[31] Nelson, B., Barreno, M., Chi, F. J., Joseph, A. D., Rubinstein, B. I., Saini, U., Sutton, C. A., Tygar, J. D., and Xia, K. 2008. Exploiting machine learning to subvert your spam filter. *LEET* 8, pp. 1–9.

[32] Ney, P., Koscher, K., Organick, L., Ceze, L., Kohno, T. 2017. Computer security, privacy, and DNA sequencing: Compromising computers with synthesized DNA, privacy leaks, and more. In *26th USENIX Security Symposium (USENIX Security 17)*, pp. 765–779.

[33] Nguyen, M. H., Le Nguyen, D., Nguyen, X. M., and Quan, T. T. 2018. Auto-detection of sophisticated malware using lazy-binding control flow graph and deep learning. *Computers & Security* 76, pp. 128–155.

[34] Noreen, S., Murtaza, S., Shafiq, M. Z., and Farooq, M. 2009. Evolvable malware. In *Proceedings of the 11th Annual conference on Genetic and evolutionary computation*, ACM, pp. 1569–1576.

[35] Pan, J., Fung, C. C. 2008. Artificial intelligence in malware-Cop or culprit? University of Western Australia.

[36] Pan, W. and Jin, Z. 2018. Edge-based modeling of computer virus contagion on a tripartite graph. *Applied Mathematics and Computation* 320, pp. 282–291.

[37] Parsaei, M. R., Javidan, R., Kargar, N. S., and Nik, H. S. 2017. On the global stability of an epidemic model of computer viruses. *Theory in Biosciences* 136, 3–4, pp. 169–178.

[38] Rad, B.B., Masrom, M., Ibrahim, S.: Camouflage in malware: from encryption to metamorphism. *International Journal of Computer Science and Network Security* 12, 8, pp. 74–83.

[39] Ren, J. and Xu, Y. 2017. A compartmental model for computer virus propagation with kill signals. *Physica A: Statistical Mechanics and its Applications* 486, pp. 446–454.

[40] Singh, J., Kumar, D., Hammouch, Z., and Atangana, A. 2018. A fractional epidemiological model for computer viruses pertaining to a new fractional derivative. *Applied Mathematics and Computation* 316, 504–515.

[41] Steels, L. 1993. The artificial life roots of artificial intelligence. *Artificial life* 1, 1–2, pp. 75–110.

[42] Stoecklin, M. P. 2018. Deeplocker: How AI can power a stealthy new breed of malware. *Security Intelligence*, August 8: https://securityintelligence.com/deeplocker-how-ai-can-power-a-stealthy-new-breed-of-malware/

[43] Szor, P. 2005. *The Art of Computer Virus Research and Defense*. Pearson Education.

[44] Tramer, F., Zhang, F., Juels, A., Reiter, M. K., and Ristenpart, T. 2016. Stealing machine learning models via prediction apis. In *25th USENIX Security Symposium (USENIX Security 16)*, pp. 601–618.

[45] Whitley, D. 1994. A genetic algorithm tutorial. *Statistics and computing* 4, 2, 65–85.

[46] Xu, W., Qi, Y., and Evans, D. 2016. Automatically evading classifiers. In *Proceedings of the 2016 network and distributed systems symposium*, pp. 21–24.

[47] Zelinka, I. 2004. SOMA – self organizing migrating algorithm. In *New optimization techniques in engineering*, Springer, pp. 167–217.

[48] Zelinka, I., Das, S., Sikora, L., and Senkerik, R. 2018. Swarm virus-next-generation virus and antivirus paradigm? *Swarm and Evolutionary Computation* 43, 207–224.

[49] Zelinka, I. and Jouni, L. 2000. SOMA – self-organizing migrating algorithm. In *Mendel 2000, 6th International Conference on Soft Computing*, Brno, Czech Republic, pp. 177–187.

[50] Zhang, X. and Gan, C. 2018. Global attractivity and optimal dynamic countermeasure of a virus propagation model in complex networks. *Physica A: Statistical Mechanics and its Applications* 490, pp. 1004–1018.