Machine learning and automation in cybersecurity

By Jake Whamond c3327794

Word count 3834

Exec summary

Cybersecurity about machine learning and automation has several promising areas: automated/ machine learning vulnerability discovery, Fuzzing, Botnets and sensitive information, and automated and machine learning in the Cyber Kill Chain framework. The use of machine learning and automation in the 2022 Ukraine-Russian war, particularly phishing cyberattacks. Many types of machine learning exist. With the increasing involvement of cyberspace in war, innovation in the field is likely to increase. However, there are limitations in machine learning and automation, making a human always needed. The limitations, particularly in attacks that are not easily predicted, such as the case of threats from the inside.

Table of contents

1. Title page
2. Executive summary
3. Table of contents
4. Introduction
5. Automated/ machine learning vulnerability discovery
6. Fuzzing, Bot nets and sensitive information
7. The use of automated and machine learning in the Cyber Kill Chain framework
8. The use of automated and machine learning in cyber attacks
9. Types of potential machine learning use in cybersecurity
10. The use of machine learning and automation in the 2022 Ukraine-Russian war
11. Phishing attacks and machines learning
12. Limitations of machine learning and automation
13. Strengths and limitations of different types of machine learning
14. Summary
15. Refences

Introduction

Machine learning (ML) and automation in cybersecurity is an ever-increasing concern as skill storage in the industry become apparent, along with the ever-increasing, more skilled attacks that malicious actors do. It makes an automation response convenient and necessary to combat such actors and skill storage. Automation and Machine learning integration could be a critical change in cybersecurity, giving those in cybersecurity positions time to figure out problems not quickly done with automation or Machine learning. In contrast, automation and Machine learning does the tasks easily and quickly done with automation. Many areas, particularly.

1. Automated/ machine learning vulnerability discovery and cybersecurity defense
2. Fuzzing, Bot nets and sensitive information
3. The use of automated and machine learning in the Cyber Kill Chain framework
4. The use of machine learning and automation in the 2022 Ukraine-Russian war
5. Phishing attacks and machines learning

May need to receive an overview as automation and machine learning have radically changed or is likely to change many industries over the years.

“The key difference between traditional rule-based and machine learning systems is that machine learning systems have the capacity to learn and modify their own behavior to achieve some measurable objective.” (2)

“The automation of security enforcement systems is one of the most important techniques for enabling a fast response to security challenges, but the complexity of security management might hinder the successful achievement of the desired security.” (3)

“Advanced methods using ML are being developed to discover previously unknown cyber intrusions and techniques towards a more dependable cybersecurity infrastructure, including both defensive and offensive approaches.” (4)

Automated/ machine learning vulnerability discovery and cybersecurity defense

Software that can act on or assess threats is crucial for cybersecurity. a well-known tactic for finding the weakest link in the cybersecurity chain is to try and break in first and fix the error before other actors can find the error. Manually this can take hours. The exemplary Machine learning in Cybersecurity targeting exploits in a system could make up for the lack of cybersecurity professionals' storage in the industry, making for a more robust response to cyber-attacks. Cybersecurity professionals will be able to focus on risk and threat assessments more quickly. The ability of automated software to read extensive amounts of data and catalogue is also vital in a cybersecurity context. It allows for a human to solve the high threats and risks first. Machine learning has already combated several known types of cyberattacks with success User to Root (U2R), Denial of Service (DoS), probe attacks Remote to Local (R2l), and Remote to Local (R2l). Ransomware detection by automated software has been a research target, with at least one method being offered; this is of particular interest because of the increased attacks of this nature.

“With the increased number of ransomware-based cyber-attacks, ransomware detection methods are needed. Even though ransomware share many aspects of features with other types of malwares, some features are specific to ransomware” (1)

Graph from (1)

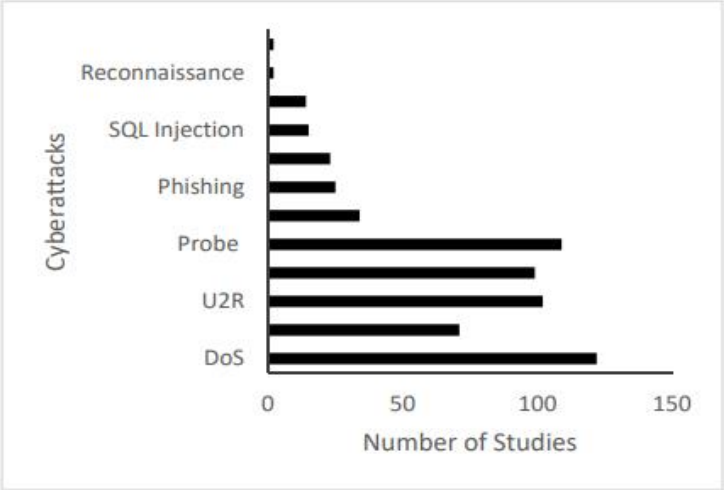

Figure 6. Cyberattacks solved by the Machine Learning (ML) techniques used in the selected reviewed papers and the number of studies that employed ML techniques to solve the different attacks.

Of course, there are some inherent errors in software as it only does what the programming tells it to do as compared to human critical thinking ability. New novel ways to exploit systems are unlikely to be handled by the software program for the traditional exploits. naturally, this makes regular updates a need instead of a want, but how regular is np-complete.

“Typically, security systems have the capability to detect malware based on the malware's signature. But the year 2018 saw incidents of attackers using machine learning to create malware signatures that security programs were not able to detect” (5)

“These tools, at least at the present time, do not develop new exploits autonomously. The hard work of writing code that exploits a previously unknown vulnerability is still largely a human-directed endeavor” (5)

Fuzzing

The fuzzing technique one of the ways automated software is used in cybersecurity. In this instance, fuzzing does vulnerability discovery break-in before other actors do.

“Compared with other techniques, fuzzing is easy to deploy and of good extensibility and applicability, and could be performed with or without the source code” (6)

stages of fuzzing

- testcase generation stage
  the generation of testcases the created cases determined the quality of the fuzzing test
- testcase running stage
  test cases run
- program execution state monitoring
  test cases either causes problems or not in the program
- analysis of exceptions
  analysis of any problems

“As an automated method for detecting vulnerabilities fuzzing has shown its high effectiveness and efficiency.” (6)

“Fuzzing in vulnerability discovery techniques is an efficient method to discover the software weaknesses” (6)

Bot nets

Frequently used as an automated way by bad actors to do DoS attacks, denial of service (dos attacks), and phishing attacks. one of the largest if not largest and most effective DoS attacks was done by a botnet malware called Mirai, a self-propagating worm infecting thousands of systems by employing automation scanning looking for a particular vulnerability. versions of Miria still exist to this day, but the most significant attacks were in 2016.

“Mirai takes the following two stages. The first is the infection stage. Mirai searches for an IoT device using port 23 or 2323. Once Mirai finds such a device, it tries to log-in with easy-to-guess passwords. If succeeding in log-in, Mirai downloads an architecture-dependent code from the Command and Control (C&C) server and executes it. As a result, the device becomes a bot. The second is the attack stage. Once an attacker issues a command, the C&C server delivers it to bots. All the bots begin a DDoS attack on the target specified by the attacker” (7)

Sensitive information

It is also essential that such automated software recognise sensitive information regarding individuals or organisations. Further sensitive information often depends on that definition by the context in a specific situation that is often overlooked by an automated software as the software is often looking for keywords, not the context.

“Existing research efforts on identifying sensitive data from its descriptive texts focus on keyword/phrase searching. These approaches can have high false positives/negatives as they do not consider the semantics of the descriptions.” (8)

The use of automated and machine learning in the Cyber Kill Chain framework

Reconnaissance

Scouting for vulnerabilities is one way to scan automated tools to assess large data sets. It may also be possible to use machine learning to add strength to such tools.

“Attackers can use more active techniques, such as automated scanners that probe target networks for details on their connected systems, network defenses, and associated software configurations.” (5)

Weaponization

The weaponization of the automated tools can prove a danger to systems vulnerable to known types of cyber-attacks as the methods of the attacks could be taught using machine learning.

“Automated weaponization tools can rapidly identify vulnerabilities and assemble code to exploit them. These tools often feature databases of exploits that attackers can search through to find ones that suit their target’s apparent vulnerabilities” (5)

Delivery

Automated Delivery scales up the effects as opposed to manual delivery technology.

“More than 90 percent of all detected malicious code was initially delivered via email, and that spear phishing—which remains a largely manual process” (5)

“in 2016, Russian military intelligence operatives targeted key members of the Democratic National Committee and John Podesta, chair of Hillary Clinton’s presidential campaign. The scale of the effort, which featured more than 9,000 spear phishing links, illustrates both the perceived value of the technique as well as the decision calculus of phishing with so many spears: send out a large number of targeted emails and hope a few unsuspecting users take the bait” (5)

Command and control

Control and command(C2) malicious code that slips past the defence vulnerability of systems needs to be controlled by the actor that put it there to activate. automation could make this less essential or op delete it together

“C2 may also persist as a failsafe function for malicious attack code; in the event of an error or environment that the malicious code cannot process through its other automated functions” (5)

“In 2008, Conficker, a virulent computer worm, signaled the beginning of a new era. It was the first well-publicized instance of malicious code utilizing C2 infrastructure that was not hard coded with a preset directory of domains to check.The first version of Conficker used an algorithm to generate pseudo-random domain names for C2” (5)

Pivoting

Pivoting successful malicious code into other systems, machine learning can prove critical to doing this and, as such, offer how such attacks might be defended potentially with machine learning.

“A famous example was a worm, known as Agent. BTZ, that infected both unclassified and classified United States military networks in 2008. Attackers used USB drives with malicious code that self-

propagated and caused a significant number of infections.In this attack, infected systems compromised USB drives connected to them, and then the drives infected additional systems when connected elsewhere" (5)

Action and objective

The activation of malicious code has several different objectives, from fining financial or private information. Various objectives can also include attacking personal or organisation/government rivals

"Russian attackers launched a new piece of malicious code called CRASHOVERRIDE. * CRASHOVERRIDE was meant to substantially automate the attack process: its core module could automatically find circuit breaker controls and toggle them on and off, creating a blackout. Analysts also noted that the malicious code could be easily adapted to other power grid systems in Europe, the Middle East, Asia, and the United States. In effect, the creators of CRASHOVERRIDE had developed an automated weapon that they could easily adapt for electrical grids all over the world" (5)

The use of automated and machine learning in cyber attacks

Machine learning and automation can also use for attacks; as previously discuses in the cyber security kill chain, this represents a significant cybersecurity threat. If not countered, the purpose scale of such attacks will likely affect millions more than the traditionally used manual malware. Due to this increasing machine learning and automated attacks, it is necessary to look further into the field.

"Machine learning is commonly known to assist in the detection of cyber threats. However, attackers are using machine learning to facilitate cybercrime. Trends show that machine learning is being used to create sophisticated malware that can bypass an organization's security systems. Tracking machine learning enhanced cyber threats allows organisations to stay informed of the different ways that machine learning is being used to facilitate crime" (5)

Types of potential machine learning use in cybersecurity

Supervised machine learning as means of defense and attack

Feeding data to programs that then can learn from those data sets is a valuable tool for both defenders and attackers as the defender can easily assess threats and risks. The attacker will be able to find worthwhile targets faster

“Supervised learning can also help both defenders and attackers with an important question: which vulnerabilities are worth exploiting? Defenders will want to prioritize their security efforts to remediate these weaknesses. Attackers will want to exploit the most damaging of these flaws in the weaponization and delivery steps of the kill chain” (5)

” These barriers, such as anti-virus systems, intrusion detection systems, Center for Security and Emerging Technology spam filters, and other defenses often use machine learning. While the earliest spam detection rules-based systems were easily beaten once attackers learned the rules—such as rewriting “free” as “F*R*E*E” to avoid being classified as spam—modern machine learning cyber defense systems are more flexible and harder to evade” (5)

Generative learning in cybersecurity

perhaps the closest thing to artificial intelligence this proves to have potential in cybersecurity as it could come up with solutions to novel attacks in real-time a limitation in the field currently Generative learning could also make more effective honeypots for the bad actors could fall into rather than attacking legitimate business/organisations

“These generative learning systems can create very realistic-seeming snippets of text, video, or audio. Among many other achievements, they can create “deepfake” images and video and write complex text on the fly” (5)

Trial and error machine learning

Trial and error machine learning is a perfect tool for vulnerability discovery. This machine learning can quickly discover any vulnerability by simply running the gauntlet of trying to break into the program again and again much faster and more effectively than the average human.

“These newer defenses are, however, vulnerable to attacks by adversarial learning systems” (5)

“These types of adversarial approaches will make defense evasion significantly easier for attackers” (5)

The use of machine learning and automation in the 2022 Ukraine-Russian conflict

The current cyber-attacks between Ukraine and Russia and their use of machine learning and automation in such state-sponsored attacks might signal a new wave of innovation in automation and machine learning, as conflict often does.

For instance, a wiper malware RURansom has been released. Its automation scans for a Russian IP address if the condition is fulfilled. The wiper activated such use of automation targeted attacks for any organisations or country looking to hurt a specified target could be helpful too.

Phishing attacks and machines learning

The Ukraine-Russian conflict has played large phishing attacks as a delivery mechanism for many a malware program machine learning has allowed for more significant detection of phishing attacks.

"The conventional approaches for phishing attack detection are not accurate and can recognize only about 20% of phishing attacks. ML approaches give better results but with scalability trade-off and time-consuming even on the small-sized datasets" (9)

"It the rise of machine learning solutions, these techniques were being used to fight social engineering as it can effectively detect suspicious links in emails, detect counterfeit images and videos, and flag suspicious URLs, to name a few" (9)

COMPARISON OF MACHINE LEARNING BASED PHISHING DETECTION SYSTEMS (10)

Description	Pros	Cons
• Detects phishing attacks by using a whitelist filter	• Pages that bypass the whitelist filter are filtered again by Support Vector Machines. • Maintains accuracy of whitelist filter by using a personalized whitelist.	• Limited dataset of 850 pages. Unable to detect the attachment of DNS spoofs to legitimate web pages. • High False positive rate.
• Implement a comment spam detection mechanism that can be used as a browser plugin and remove spam comments	• Balances dataset by applying WEKA filters to get the best suitable features. • Spam detection classifier can accommodate new features and detect new classes of spam content.	• Does not do well with a random dataset without applying a supervised resample filter.
• Proposes a machine learning-based method that can detect whether a web page exhibits phishing attacks	• Proposed method is based on an easy to acquire feature vector that does not require additional computation.	• Only uses 10 features for detection. • Limited dataset of 1353 instances.
• Uses feature selection to identify important features that categorize phishing and legitimate websites.	• Feature selection highly improves the accuracyscore after implementation. • Use of feature selection reduces computational time.	• 14 features. • limited dataset (200 legitimate URL and 400 phishing URL) • May not work properly with datasets of equal URLs of legitimate and phishing web pages.
• Builds a system using machine learning that can classify websites using URLs.	• Can be used to build a rule-based system with associative rules to classify URLs.	• 9 features for each URL • All features are discrete • Limited dataset (1353 URLs)
• Proposes a learning-based aggregation analysis mechanism to decide page layout similarity, which is used to detect phishing pages	• Automatically trains classifiers to determine web page similarity from CSS layout features, which does not require human expertise.	• Method is lightweight as it only takes one class of features, CSS structure. • Limited by the size of the dataset and distribution of samples.
• This research uses a new attribute called the "domain top page similarity" to improve the efficiency of a machine learning-based phishing detection model	• Increases f-measure and reduces the error rate. • Proves that with better features, the detection rate is much higher and can be implemented in future works.	• The model is highly dependent on the accuracy of the features.

• This paper proposes a real-time anti phishing system that uses seven classification algorithms and natural • language processing-based features (NLP)	• Independence from language and third party • services. • Huge dataset of legitimate and phishing data. • Real-time execution. • Can detect new websites because of NLP features	• Machine learning-based systems cannot correctly utilize such a vast dataset.
• Performs an extensive measurement of squatting phishing, where the phishing pages impersonate target brands at both the domain and content level.	• Uses features from visual analysis and optical character recognition. • Open-sourced tool. • Uses evasive behaviors of phishing pages to build classifiers.	• Unable to detect phishing pages that use cloaking. • Only focuses on popular brands. • The classifier cannot be compared with other phishing tools like CANTINA and CANTINA+
• Uses features from HTML content • JavaScript code and URLs to build a classifier that can detect malicious web pages and threat types	• Diverse features. • High accuracy score. • Highlights features that are necessary to extract.	• Limited dataset (2500 URLs) • Classifier may not do well with large datasets.

Limitations of machine learning and automation

Detection from the threats inside organisations are a great limitation in the use of machine learning and automation as there no set pattern or data set when individual humans are directly involved making models hard to make as people will act or react differently from each other even serotypes are often wrong the difference between an ageing technology literate employee and a young technology illiterate employee

“Insider threat behaviour and network activity is often difficult to model because it is unpredictable and constantly changing” (11)

(11) machine learning techniques

Machine learning	Strength	Limitation
Random forest	Ability to classify network intrusion threats more accurately than other machine learning classification algorithms like decision tress and work better on a large dataset	Random forest can generate many noisy trees which impacts the accuracy and decision making of the classification
Decision tree	Decision tress are but powerful algorithms which have been reported to identity security features within a network that indicate malicious activity i.e. misuse intrusion as well as small variation in known attacks	Model training time tedns to be high for decision tree classifiers due soace complexities
Artificial neural network	Can effectively detect known attacks like Denial of service and variants due to patterns recognition and has a high fault tolerance	When the neural network does not behave as expected for example not detecting a DoS threat it will put forth a solution was proposed which can affect trust in the neural network
K-nearest neighbor	Effective for classification of cyber threats as it groups attacks into clusters and classifiers new attacks into the most applicable cluster based on training data	Computation cost is high as the proximity/distance must be calculated between each neighbor for every value this algorithm becomes impractical when a large data set of cyber threats must be analyzed

Summary

Cybersecurity work with machine learning and automation has several optimistic areas, mainly automated/ machine learning vulnerability discovery, Fuzzing, Botnets and sensitive information, and automated and machine learning in the Cyber Kill Chain framework. The use of machine learning and automation in the 2022 Ukraine-Russian war, particularly phishing cyberattacks. Many types of machine learning exist. With the increasing involvement of cyberspace in war, innovation in the field is likely to increase. However, there are limitations in machine learning and automation; making a human always needed the limitations, particularly in attacks that are not easily predicted, such as the case of threats from the inside. Several automation and machine techniques are already used in Cybersecurity, including Random Forest, K-nearest neighbor, Artificial neural network, Decision tree, fuzzing, and bots. The use of machine learning in detecting phishing attacks and other cyberattacks could be significantly increased. Generative learning, Trial and error and Supervised machine learning all offered promising approaches in the field

Fw_ Adverse Circumstance Applicat

Refences

(1) Bae, S., Lee, G. and Im, E., 2019. Ransomware detection using machine learning algorithms. Concurrency and Computation: Practice and Experience, 32(18).

(2) V. Moreno, G. Génova, E. Parra and A. Fraga, "Application of machine learning techniques to the flexible assessment and improvement of requirements quality", Software Quality Journal, vol. 28, no. 4, pp. 1645-1674, 2020.

(3) D. Rivera, F. Monje, V. Villagrá, M. Vega-Barbas, X. Larriva-Novo and J. Berrocal, Automatic Translation and Enforcement of Cybersecurity Policies Using A High-Level Definition Language, Entropy, vol. 21, no. 12, p. 1180, 2019.

(4) I. Aiyanyo, H. Samuel and H. Lim, "A Systematic Review of Defensive and Offensive Cybersecurity with Machine Learning", Applied Sciences, vol. 10, no. 17, p. 5811, 2020.

(5) B. Buchanan, J. Bansemer, D. Cary, J. Lucas and M. Musser, "Automating cyber Attacks hype and Reality", Cset.georgetown.edu, 2022. [Online]. Available: https://cset.georgetown.edu/wp-content/uploads/CSET-Automating-Cyber-Attacks.pdf. [Accessed: 18- May- 2022].

(6) J. Li, B. Zhao, and C. Zhang, “Fuzzing: a survey,” Cybersecurity, vol. 1, no. 1, Jun. 2018, doi: 10.1186/s42400-018-0002-

(7) S. Yamaguchi, “White-Hat Worm to Fight Malware and Its Evaluation by Agent-Oriented Petri Nets,” Sensors, vol. 20, no. 2, p. 556, Jan. 2020, doi: 10.3390/s20020556.

(8) Z. Yang and Z. Liang, “Automated identification of sensitive data from implicit user specification,” Cybersecurity, vol. 1, no. 1, Sep. 2018, doi: 10.1186/s42400-018-0011-x.

(9) A. Basit, M. Zafar, X. Liu, A. R. Javed, Z. Jalil, and K. Kifayat, “A comprehensive survey of AI-enabled phishing attacks detection techniques,” Telecommunication Systems, Oct. 2020, doi: 10.1007/s11235-020-00733-2.

(10)S. Hossain, D. Sarma, and R. Joyti, “Machine Learning-Based Phishing Attack Detection,” International Journal of Advanced Computer Science and Applications, vol. 11, no. 9, 2020, doi: 10.14569/ijacsa.2020.0110945.

(11) J. Scott and M. Kyobe, "Trends in Cybersecurity Management Issues Related to Human Behaviour and Machine Learning," 2021 International Conference on Electrical, Computer and Energy Technologies (ICECET), 2021, pp. 1-8, doi: 10.1109/ICECET52533.2021.9698626.