A note on machine learning applied in ransomware detection

Manuela Horduna[1], Simona-Maria Lăzărescu[1], and Emil Simion[2]

[1] University "Alexandru Ioan Cuza" Iasi, Faculty of Computer Science

[2]Polytechnic University of Bucharest

Abstract

Ransomware is a malware that employs encryption to hold a victim's data, causing irreparable loss and monetary incentives to individuals or business organizations. The occurrence of ransomware attacks has been increasing significantly and as the attackers are investing more creativity and inventiveness into their threats, the struggle of fighting against ill-themed activities has become more difficult and even time and energy-draining. Therefore, recent researches try to shed some light on combining machine learning with defense mechanisms for detecting this type of malware. Machine learning allows anti-ransomware systems to become more accurate at predicting outcomes or behaviors of the attacks and is vastly used in the advanced research of cybersecurity. In this paper we analyze how machine learning can improve malware recognition in order to stand against critical security issues, giving a brief, yet comprehensive overview of this thriving topic in order to facilitate future research. We also briefly present the most important events of 2022 in terms of ransomware attacks, providing details about the ransoms demanded.

Keywords— Ransomware, machine learning, malware, cybersecurity

1 Introduction

Malicious software, shortly malware, is software designed to corrupt or damage a system. We can classify malware based on payload, the way it propagates, or other execution features, and its targets can be individuals, companies, or institutions. The principal types of malware are worms, trojans, viruses, botnets, adware, and ransomware. The COVID-19 pandemic had an important role in the increase in the cyberattack rate because the attackers use this context to spread ransomware through phishing emails. In the middle of the year 2021, The HHS Cybersecurity Program specified that 48 of the 82 global ransomware attack cases reported up to that time targeted the US Healthcare entity.

Ransomware is a form of malware which have the objective to prevent access to personal information until a ransom will be paid, most often being required cryptocurrency such as Bitcoin for the ransom in order to make it even more difficult to track the transactions. May 2021 represented an important moment in terms of the importance of paying the ransom because it brought to attention the discussion of whether or not the payment of ransom should be made to the attackers. At that time almost $5 million or the equivalent of 75 Bitcoins were paid to the DarkSide group by Colonial Pipeline to release their affected computer system. Paying the ransom can further encourage cybercriminals to carry out such attacks. For this reason, this payment of the ransom could soon become illegal, because there is a legislative framework in the United States that is taking shape in this regard. The capability to analyze a large amount of data fast makes machine learning algorithms an adequate and useful mechanism in ransomware, and more generally malware, detection.

Nowadays, ransomware is more sophisticated with every attack that appears, but it has its origins in 1989 when one of the first ransomware attacks, called the AIDS trojan, was documented. AIDS Trojan used symmetric cryptography, it was released through a floppy disk and the victims had to pay $189 in order to regain access to their systems.

2 Retrospective of ransomware attacks in 2022

The year 2022 brings to light the fact that paradoxically, although the number of ransomware attacks remains a significant one, the affected victims paid approximately 16 million dollars compared to 74 million dollars in 2021, which represents a percentage of only 22%. It is not yet possible to say exactly what generated these things, but it is suspected that a certain role was also played in the context of May 2022 when the Conti ransomware group, one of the most notorious cybercrime collectives, shouted down their operation and infrastructure.

- **January 2022**

  The year 2022 started from the first month with important events regarding ransomware attacks. In addition to attacks targeting the government area in states such as New Mexico or Pennsylvania (Crawford County), companies were also targeted. In the case of Thales Group, the French aerospace giant, no ransom request was received, and LockBit claimed the responsibility for this attack. The Conti criminal group attacked a transportation and logistics company in Minnesota called Bay & Bay Transportation. The company is not at the first such incident, the first taking place in 2018 when it had to pay the ransom, and thus it was able to return to 90% of its activity in two and a half days without paying a ransom this time. Ransomware attacks also hit the education and health areas, a serious case being that of the Department of Health in Maryland where hospitals were affected in the context of a new wave of COVID-19 cases. Even in this case no ransom was paid and the importance of not paying any such demands was even emphasized

- **February 2022**

  The month of February continues with attacks on educational institutions, such as the case of the Ohlone Community College District from California, but also with several attacks from the Conti and BlackCat groups. Conti carried out attacks on KP Snacks, a British snack producer from the UK (where he managed to affect the distribution of products to supermarkets and gain access to information such as credit card statements or employee personal data), New Zealand Uniforms (in which case they did not no ransom was paid, and the systems became functional again in two days), Cookware giant Meyer (where employees' personal information was obtained) or University of Neuchâtel, Switzerland. As for BlackCat, their targets were two German oil companies, Oiltanking Group and Mabanaft Group, which share a parent company called Marquard & Bahls, and also the Zurich-based airport services giant Swissport. Another important event was represented by the San Francisco 49ers attacked by BlackByte ransomware before the Super Bowl. Also, Nvidia was attacked by the Lapsus$ hacking group.

- **March 2022**

  In March, a new target was represented by the Toyota company, which had to stop production in 14 factories in Japan, shortly followed by Denso Automotive, one of the largest manufacturers of auto components in the world. The Lapsus$ hacking group targets Samsung, Vodafone, and the French video game company, Ubisoft. Microsoft was also affected by an attack from the Lapsus$ group. Through Ronin's Axie Infinity mobile game, a new attraction in the crypto community that allows you to earn digital coins and NFTs during Pokemon-style battles, hackers managed to earn at least $625 million dollars in cryptocurrencies.

- **April 2022**

  For the month of April, one of the major events was the attack on the Coca-Cola company by Stormous. The attackers demanded the sum of 64,000$ (equivalent to £51,000), i.e. approximately 1.65 Bitcoin, on the dark web for the 161 gigabytes of stolen data. Also, Conti targets the industrial giant Parker Hannifin and the automotive tools manufacturer and designer Snap-on Incorporated. There are also attacks on the Government of Costa Rica, at which time a country declares for the first time a national emergency in response to a cyber-attack. In a first instance, Conti group is asking for a ransom of $10 million, going to increase the ransom to $20 million.

- **May 2022**

  The month of May returns with attacks on the country of Costa Rica, this time the attack is carried out by HIVE on Costa Rica's public health service. An attack on Glenn County Office of Education and school districts, California was reported on May 12 by Sacramento Valley Mirror (SVM) by Quantum Group. On June 7, the amount of $400,000 was sent by the Glenn County Office of Education to Quantum in a BTC wallet to obtain the decryption key. It is important to state that Quantum's initial demand was well over $1 million.

- **June 2022**

  In the month of June, there were several attacks on Italy. On the one hand, when the city of Palermo was hit by the Vice Society ransomware and 1.3 million people were affected, and on the other hand, when the University of Pisa was hit by Black Cat and was a ransom of $4.5 million was requested if the payment was made by June 16th, otherwise, the ransom will increase to $5 million.

- **July 2022**

  July catch the BlackByte Group attacks on Lamoille Health Partners from Vermont and Gateway Rehab, Pennsylvania. LockBit hits the French virtual mobile telephone operator La Poste Mobile on July 4, affecting its administrative services. Black Cat hits this time the Japanese multinational video game publisher called Bandai Namco. Italy is also affected this time, now at the Agenzia Delle Entratede or Italy's tax office, by LockBit who threatens to publish 100Gb of stolen data on the dark web if payment is not made by August 1st. A ransomware attack carried out by HIVE also affects Wooton Upper School in Bedfordshire, UK, and a ransom of £500,000 is demanded.

- **August 2022**

  August also comes with a multitude of ransomware attacks. The infrastructure from the Center Hospitalier Sud Francilien located in Paris, France was compromised and a ransom of $10,000,000 was demanded to receive the decryption key. A ransom of $10 million was also requested by the Cuba ransomware gang after the attack on the Parliament of Montenegro. A much smaller amount this time, of only $600,000, was requested by Quantum who was behind the attack of the Instituto Agrario Dominicano from the Ministry of Agriculture in the Dominican Republic.

- **September 2022**

  September highlights the attack on the Australian company Optus during which the data of 10 million customers were stolen and a ransom of $1 million in the Monero cryptocurrency was demanded. There is a $5 million ransom demanded this time by BlackCat to decrypt Wheat Ridge's municipal data and computer systems. Also in September, the attack carried out by the HIVE Group on Tift Regional Medical Center, Georgia was made public. The attack occurred on July 14, and on August 25, HIVE sent an email to Tift Regional Medical Center to begin negotiations. On August 26, HIVE asks for the amount of $1,150,000.00, and on September 2, the negotiator from the medical center counter-attacks the hackers' offer and offers them the amount of $100,000 instead.

- **October 2022**

  One of the major events that marked the month of October 2022 was the attack on the Pendragon Group from the UK by LockBit when a record amount was requested as a ransom, namely the amount of $60 million. Another important attack also carried out by LockBit was that of Brazil's BRB Bank. The ransom requested this time was 5.2 million Brazilian reals, which is the equivalent of 50 BTC. In the same month, LockBit also targets Oomiya, a Japanese technology company, and Kingfisher Insurance company. Also, the car manufacturer Ferrari was hit by RansomEXX.

- **November 2022**

  The month of November is marked by other attacks carried out by LockBit, one of them on the French company Thales and on the multinational automotive group Continental from Germany. In the case of the Continental company, the stolen data was put up for sale for $50 million. LockBit is also demanding $2 million to destroy the data stolen from the Kearney & Company or $10,000 to extend the time for another 24 hours.

- **December 2022**

  In the last month of 2022, we note the Royal ransomware attack on the American telecommunications company called Intrado. In this case, the requested ransom amounted to $60 million. LockBit hits again, this time on the Port of Lisbon, Portugal. This time, a ransom of $1.5 million, which has a payment deadline of January 18, is being confused.

3 Ransomware Classification

There are five general classes of ransomware: locker ransomware or screen locker, crypto-ransomware or data locker, leakware, scareware, and ransomware as a service (RaaS).

Locker ransomware. A locker ransomware has a low level of risk and aims to block almost complete access to computing resources, allowing the victim to interact with the device only to pay the ransom. Because of the fact that only the interface is locked, which means that the mouse and keyboard can only be used for payment, and the data is not encrypted, the victim can remove this type of ransomware using various antivirus software.s

Crypto ransomware. Crypto ransomware is one of the most common types of ransomware and presents a high-risk level. This time, the victim's data and files, sometimes including the victim's backups, will be encrypted and there will be a ransom payment request for the victim to receive the decryption key.

Leakware. Also known as Doxware, leakware presents a high-risk level because it is well-targeted to institutions like banks or those who work with confidential and important data. This ransomware does not destroy the data but threathens to release the data on the public domain. Also, since the context can create damage to the image of the institution, an even greater emphasis can be placed on the quick payment of a ransom.

Scareware. Scareware has a very low level of risk and uses social engineering techniques in order to trick the user to download and install malware on their systems. It is displayed a pop-up message alert that looks legitimate which says that a problem occurred on the victim's computer and it has to be solved immediately or they were infected with malware. But in reality, is nothing more than another trying to get a ransom from the victim.

Ransomware-as-a-Service. Ransomware-as-a-service is based on affiliate schemes or networks that permit earning a percentage of the ransom payment to all the persons who have low technical knowledge about how to create ransomware, but who are members of this network. It is only necessary that those members spread the ransomware as far as possible, while the RaaS vendor can focus on how to make this malicious software make the damage even more.

4 Propagation methods

There are multiple possible ways in which ransomware is able to get into a system. The following list with methods included is not exhaustive, since the rise of ransomware-as-a-service is making it easier than ever for every novice criminal to be able to launch their own customized attacks.

- **Phishing campaigns which contain malicious links or attachments.** One of the most common ways to spread the ransomware is through email. The attacker designs an email pretending to be from a credible source (e.g. Human Resources or Information Technology department) and attaches a malicious file in a Microsoft Word or similar document file that is embedded with malicious macros. These macros execute malware upon download.
- **Exploiting vulnerabilities in software.** There are a wide variety of potential software vulnerabilities, but most of them fall into a few main categories: buffer overflows, invalidated input, race conditions, access-control issues, weakness in authentication, authorization, or cryptographic practices.
- **Cross-Site Scripting** XSS attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Legitimate websites can have malicious scripts injected into their site that can redirect traffic to malicious websites.
- **Malvertising campaigns.** It is a technique that injects malicious code within digital ads. It is difficult to detect by both internet users and publishers and the infected ads are usually served to consumers through legitimate advertising networks. Because ads are displayed to all website visitors, every page viewer is at risk of infection.
- **Smishing** is a phishing cybersecurity attack carried out over mobile text messaging. Smishing text messages are often disguised to be from a bank, asking for personal or financial information such as personal account or ATM number.
- **Use of botnets for malicious purposes.** A botnet is a collection of devices that have been infected with a bot program that allows an attacker to control them. A device can only be involuntarily roped into a botnet if an attacker can gain access to it - first, to plant the bot and subsequently to issue commands to it. Aside from the most common way to form a botnet with desktop computers, botnets can be created from devices such as IP cameras (Persirai botnet), Routers (Mirai botnet), Android mobile devices (WireX botnet). The botnet program will usually try to contact a remote website or server where it can retrieve instructions given by the attacker.
- **Self-propagation capabilities** This technique represents a wormlike behavior by spreading infected files to all contacts available at that machine. ZCryptor is the first that has emerged from self-propagation behavior on the Windows platform.

Some of the main ransomware attacks with their propagation methods are described in the following table:

Name	**Type**	**Main propagation Method**	**Year**
Lapsus	Locker	Voice Phishing, Supply chain	2022
Conti	Crypto	Phishing emails	2021
Nefilim	Locker	Phishing emails	2020
Maze	Crypto	Phishing emails, Remote desktop connection password cracking	2019
REvil	Crypto	Phishing emails, Remote desktop connection password cracking	2019
Ryuk	Crypto	Phishing emails	2018
WannaCry	Crypto	ExternalBlue exploit	2017
Petya	Locker	Phishing emails	2016
Fantom	Locker	Uses a fake Windows update screen	2016
Mischa	Crypto	Gain administrative privileges through exploiting vulnerabilities	2016

Table 1: Main ransomware attacks with their propagation methods

5 Ransom payment methods

The easiest way out for a victim is paying the ransom, even if it is not always a guarantee that they will recover all the data and be able to resume to normal operations.

- **Cryptocurrency**

Cryptocurrency has unfortunately fueled the rise of cybercrimes. It has two key aspects to it: it is anonymous and non-reversible. Anonymous payment services like Bitcoin make ransomware payments simple for victims and risk-free for the ransomware owners. Early ransomware was primitive in terms of demanding payment: Premium rate SMS message extortion was very common.

Bitcoin remains the most popular payment method, but the trend is to move away from Bitcoin to cryptocurrencies such as Monero, which offers better security, privacy, and anonymity. Transactions can't be traced back to any particular user or address and histories are also kept private. Other cryptocurrencies on the rise for ransomware payments are Ethereum and Zcashiv. Both Ethereum and Zcash offer privacy and obscurity in transactions which makes them well-suited to extortion.

Ethereum is a distributed public blockchain network. There are some significant technical differences between Bitcoin and Ethereum, the most important distinction to note is that they differ substantially in purpose and capability. Bitcoin offers one particular application of blockchain technology, a peer-to-peer electronic cash system that enables online Bitcoin payments. While the Bitcoin blockchain is used to track ownership of digital currency (bitcoins), the Ethereum blockchain focuses on running the programming code of any decentralized application.

HC7 The first ransomware to accept Ether cryptocurrency as ransom payment was HC7. First observed on December 1, 2017, the Hc7 Ransomware is delivered using spam email messages, which will include a compromised attached document. These email attachments tend to take the form of Microsoft Word documents with bad scripts, which download and install the Hc7 Ransomware onto the victim's computer. Once installed, the Hc7 Ransomware will try to take the victim's files hostage, encrypting these files with a robust encryption algorithm and then demanding the payment of a ransom in exchange for the decryption key that will restore the affected files.

The Hc7 Ransomware will scan the victims' drives for the user-generated files using a strong encryption algorithm to make the affected files inaccessible. The decryption key that will restore the affected files, is sent to the Hc7 Ransomware's Command and Control servers, out of reach of the victim or their security software. The file types that are typically encrypted by attacks like the Hc7 Ransomware are: .3dm, .3g2, .3gp, .7zip, ..jar,

.java, .jpeg, .jpg, .js, .m3u, .m3u8, .m4u, .max, .mdb, .mid, .mkv, .mov, .mp3, .mp4, .mpa, .mpeg, .mpg, .msg, .pdb, .pdf, .php, .plb, .pmd, .png, .pot, .potm, .potx, .ppam, .ppj, .pps, .ppsm, .ppsx, .ppt, .pptm, .pptx, .sql, .svg, .swf, .tif, .txt, .wav, .wma, .wmv, .wpd, .wps, .xla, .xlam, .xll, .xlm, .xls, .xlsb,.xlw, .xml, .zip.

The Hc7 Ransomware will mark the files it targets in its attack with the file extension '.GOTYA,' which is added to the end of the file's name.

- **Other Untraceable Methods**

Some ransomware (for example Flocker) instead of demanding payments via bitcoins, rather asks for iTunes gift cards. Some ransomware demand payments using Paypal, MoneyPak, or by giving some email addresses and sending instructions over there.

When FLocker infects an Android Smart TV, it will lock the TV's screen and display a message from a real or fake law enforcement agency accusing the victim of committing a crime. The current FLocker variant demands a ransom to unlock the TV. FLocker can easily collect information from the TV, such as location data, phone numbers, contacts, uploaded photos, and potentially private information that the apps on your TV have permission to access.

ZCrypt ransomware creates an HTML file called 'How to decrypt files and places it in each folder containing the encrypted files. The HTML file contains a message with all details about the encryption. It is stated that data has been encrypted and that the victim must pay a ransom of 1.2 Bitcoin to restore it. In addition, if the victim does not pay within four days, the size of the ransom will increase to 5 Bitcoins. If the ransom is not paid within seven days, the private key will be destroyed and decryption will become impossible.

Unlike other ransomware-type viruses, zCrypt does not provide payment instructions - it simply encourages users to search the Internet for 'How to Buy Bitcoins' and provides an address to where payment should be sent.

One additional side note is that cybercriminals are always quick to jump in every opportunity the market has to offer. As a consequence of the mobility and flexibility of the cryptocurrency stock exchange, it is very probable that the payment methods will change too and will appear in other ways that will allow the cashing out of ransom easily and more important for the attacker anonymously.

6 Ransomware detecting models

Victims of a ransomware attack could be saved if the detection takes place before the encryption process starts. Therefore, detection plays a vital role in protection from ransomware attacks. In order to build an effective solution, it is required a study of all the available solutions for ransomware detection.

Machine learning has a great impact on the cybersecurity field because it has numerous applications to detect intrusion, fraud, malware, ransomware, and benign programs. Machine learning approaches are effective also in detecting hidden patterns.

There are several trigger patterns that could be taken into consideration when trying to detect whether a ransomware attack is launched or not:

- Opening of many files
- Structure of input and output streams to a process is different
- Many write/overwrite operations
- A process calling encryption APIs
- Frequent reading and rewriting/deleting requests in a short period of time
- Communication with a command-and-control server

- Change in the user registry keys

According to [5], the ransomware life cycle attack model could be classified in several stages, but depending on the specifics of every attack, some of them may differ:

- Finding a target
- Distribution of the infection vector
- Installation of ransomware
- Encryption key generation and retrieval
- Accessing legitimate files
- Encryption
- Post Encryption operations
- Demanding Ransom

An effective security practice uses a combination of expertise and technology to detect and prevent malware. Malware detection techniques include:

1. Signature-based detection

Signature-based detection uses known digital indicators of malware to identify suspicious behavior. Lists of indicators of compromise (IOCs), often maintained in a database, can be used to identify a breach.

2. Static file analysis

Static file analysis consists in examining a file's code, without running it, to identify signs of malicious intent. File names, hashes, strings such as IP addresses, and file header data can all be evaluated to determine whether a file is malicious. While static file analysis is a good starting point, proficient security teams use additional techniques to detect advanced malware that can go unidentified during static analysis. Using static file analysis the encryption of files could be prevented by stopping the attack before the execution moment. Another advantage of this technique is the low rate of false positives. Unfortunately, this method is time-consuming if it is done manually.

3. Dynamic malware analysis

Dynamic malware analysis executes suspected malicious code in a safe environment called a sandbox. This closed system enables security professionals to watch and study the malware in action without the risk of letting it infect their system or escape into the enterprise network.

4. File extensions blocklist/blocklisting

File extensions are letters occurring after a period in a file name, indicating the format of the file. This classification can be used by criminals to package malware for delivery. As a result, a common security method is to list known malicious file extension types in a "blocklist" to prevent unsuspecting users from downloading or using the dangerous file.

5. Application allowlist/allowlisting

Allowlisting is the opposite of a blocklist/blocklisting, where an organization authorizes a system to use applications on an approved list. Allowlisting can be very effective in preventing wicked applications through rigid parameters. However, it can be difficult to manage and can reduce speed and flexibility for the organization.

6. Malware honeypot/honeypot files

A malware honeypot mimics a software application or an application programming interface (API) to draw out malware attacks in a controlled, non-threatening environment. Similarly, a honeypot file is a decoy file to draw and detect attackers. Regarding the disadvantages of this technique, we have some false positives and we can not prevent the encryption of the files if the ransomware reaches the decoy file.

7. File entropy/measuring changes of a files' data

As threat intelligence and cybersecurity evolves, adversaries increasingly create dynamic malware executables to avoid detection. This results in modified files that have high entropy levels. As a result, a file's data change measured through entropy can identify potential malware.

8. Machine learning behavioral analysis

Machine learning (ML) is a subset of artificial intelligence (AI) and refers to the process of teaching algorithms to learn patterns from existing data to predict answers on new data. This technology can analyze file behavior, identify patterns and use these insights to improve the detection of novel and unidentified malware.

All of the above techniques can be applied also for ransomware detection that can be categorized into two major classes:

1. Misuse-based Ransomware Detection Approaches

This category uses the signatures of already discovered ransomware. It matches the encountered threat with known and available signatures to make a decision. Misuse detection can be classified depending on the nature of the signatures: structural and behavioral. In the behavioral-based detection approach, the under-examination samples are executed in a controlled environment to monitor their behavior.

2. Anomaly-based detection approaches

As a first step, a normal behavior is designed for a specific use case. Then a detection action is performed in order to discover any anomalies or malign applications that differ from the prebuilt profile.

Ransomware detection using machine learning relies on a library of malicious code features. In order to ensure a good result accuracy, the features need to be updated with as many as new discovered malicious features as possible. In recent years, researchers have widely applied machine learning techniques to detect malware through training models on a large number of features to achieve the capability of detecting new malware. That is the main reason why the latest work changed its focus on gaining more data samples and updating machine learning models to them.

7 Machine learning-based models

The rapid increased ransomware is also due to the fact that attackers started to use polymorphic techniques in order to evade detection while keeping the malicious functionality intact. Attackers may use multiple transformation techniques including register renaming, code permutation, code shrinking, and noise code insertion.

Traditional detection techniques relied on signature-based and heuristic methods, but unfortunately, these techniques were not enough to explore all the complexity of the ransomware phenomenon. In order to keep pace with the new attack variants, researchers started to focus their attention and effort on machine learning solutions, given the fact that machine learning is suited for processing large volumes of data.

As a prerequisite to understanding the benefits of machine learning techniques for ransomware detection, a workflow regarding this method is required:

1. Data gathering
2. Data preparation
3. Model building
4. Model validation
5. Model deployment

Traditional detection techniques such as Signature-based detection already mentioned in the previous section are no longer suitable for the complexity of the attacks currently existing. Also, in the case of a new type of ransomware, antivirus programs that actually use this signature-based detection may prove ineffective in these zero-day attack cases. Thus, the new trend based on machine learning algorithms began to develop more and more, in favor of detection methods that use static or dynamic analysis.

1. Support vector machines.

Support vector machines, one of the most well-known algorithms, is a technique used in malware detection to make a binary classification: malware(in our case, ransomware) or benign. It uses the idea of having a hyper-plane that splits the points from an n-dimensional space, representing our data, in two distinct classes.

The hyperplane is designed to amplify the distance between two separate classes with the maximal margin being defined as the largest distance between the examples of the two classes computed from the distance between the closest instances of both classes. Although it may seem difficult, in the context of SVMs, it is actually beneficial to work in multiple dimensions. By moving the problem to a higher dimension, the data points tend to be more easily separated, and hence there is a better chance of finding a separating hyperplane.

2. Naive Bayes.

Naive Bayes is a simple technique used for classifiers that use conditional probability from Bayes' theorem. A Naive Bayes classifier can not be used only in malware or ransomware detection but also used for spam filtering or phishing attack detection.

3. Decision trees.

The decision tree algorithm is a supervised learning technique that structures the training data in a tree and tries to make predictions for the testing data using as few decisions as possible. The most used algorithm, in this case, is ID3 and it uses the concepts of Information Gain and Entropy.

A recent paper [28] is dedicated to a new detection system that analyzes PDF documents to identify benign PDF files from malware PDF files. Portable Document Format (PDF) files are one of the most universally used file types. Like other files such as dot-com files, PNG, hackers can find means to use these normally harmless PDF files to create security threats via malicious code PDF files.

The proposed system uses the AdaBoost decision tree. The approach utilizes weights that are reallocated to each example, with higher weights allocated to incorrectly classified examples, which helps decrease bias and variance in the learning process. The assessment demonstrates a lightweight and accurate PDF detection system, achieving a 98.84% prediction accuracy with a short prediction interval of 2.174 µSec.

4. Random forests.

Random forest classifier, a supervised learning method, uses a large number of decision trees. The prediction for this method is based on the majority of the predictions obtained from each individual decision tree, meaning the prediction class with the most votes.

The classifier designed in [33] demonstrates remarkably more suited results compared to the other classifiers. The strategy adopted is based on extracting the hierarchical features in ransomware family at byte-level. Static analysis has been utilized and features are extracted directly from raw bytes of an executable file (using n-gram features). The dataset comprises three different families: Cerber, TeslaCrypt and Locky. The benign files included two types of executable files: some collected from the windows platform while the others collected from the Portable Apps platform.

The random forest prediction is based on the majority voting for the result of the combination predictions of multiple decision trees. The experimental evaluation revealed that the proposed method could achieve a high accuracy of 97.74% for the detection of ransomware.

Also, this type of classifier has several advantages[32]:

- Few input parameters are needed
- The algorithm is resistant to overfitting
- The variance decreases with increasing in the number of trees without resulting in bias

5. Genetic algorithms.

A genetic algorithm is a method that can be also applied in ransomware detection and has the goal to find optimized solutions. It has its origins in genetics, where there are taken from, for example, the notions of chromosomes representing a candidate solution or gena representing the atomic information from a chromosome, and uses procedures like crossover and mutation.

A genetic algorithm usually begins with randomly generated gene populations. Subsequently, new genes were created by taking only the selected genes according to specific criteria and recombining them in many different ways. After creating new genes through a crossover, mutations can be created with specific probabilities. This process is repeated until the termination criteria of the algorithm are met.

To solve the problem of ransomware detection using genetic algorithms, a study [47] covered this approach and concluded that the results indicate that genetic algorithm-based feature selection was useful compared to a commonly applied information gain.

According to [48], the algorithm has some disadvantages: it cannot guarantee the required solution because there are not enough rules that govern the progress. In addition, the algorithm cannot guarantee the best solution because the solution is poorly optimized. However, it has the advantages of helping secure and explore potentially substantial search spaces, finding optimal combinations, and finding solutions that are difficult to achieve.

6. Neural networks.

Neural networks are inspired by the human brain and can be used with success in malware detection. A simple neural network architecture is composed of three different layers: the input layer or the initial data, the output layer representing the result for the given data, and the hidden layer, an intermediate layer that contains the activation nodes, situated between the input and output layer.

The approach from [52] is using deep neural networks for malware detection and automatically learning features from the raw data to capture the malicious file structure patterns and code sequence patterns.

The detection process can be divided into two stages. The first stage is to preprocess malware sample data, it takes a binary form of a Windows executable file, generates a grayscale image from it, and extracts opcode sequence. This stage generates the appropriate data format as the input of the follow-up NN. The second stage applies the core process from the neuronal networks and starts learning the opcode sequence.

7. Deep leaning.

Deep learning, a subset of machine learning, has its heart in neural networks and despite the traditional machine learning methods, this method uses feature learning for the process of classification.

This approach has not received enough attention until recent years, thus more academic works are needed to explore the extents of this method.

In a recent work [53], several machine learning algorithms were implemented for the purpose of ransomware detection. Comparing the results for each of the integrated techniques, a very thorough analysis was made depending on the accuracy (the ratio of no of correct predictions to the total number of samples). The dataset includes 582 ransomware samples and 942 good ware samples. Dataset authors have collected good ware and ransomware samples from various sources and used Cuckoo sandbox for analyzing them. The method with the highest accuracy was decision trees, followed shortly by SVMs.

8 From-scratch implementations versus libraries

There are two approaches when it comes to the implementation of machine learning algorithms: the from-scratch implementation or the use of already existing libraries.

The advantages of using a from-scratch approach are the following:

- A better understanding of the mathematical aspects and how the algorithms actually work;
- The possibility of creating new algorithms or improving existing methods;
- Implicitly, a better safety and feeling of self-confidence for the one who uses such algorithms;
- It is the best solution if the project is aimed for production and you want to avoid dependencies.
- The possibility to experiment with different ways of initializing the parameters within the machine learning algorithm (for example, weights and biases).

The advantages of using already existing libraries are:

- The libraries have already been well-tested and debugged;
- It is a time-saving solution;
- The possibility of the appearance of some hidden errors is quite small.

Within neural networks and implicit deep learning algorithms, the initialization of parameters such as weights and biases plays a particularly important role because it can greatly influence the accuracy obtained in the end. Among the possibilities to initialize, for example, the weights, are:

- Initialization with zero: In this case, if we take the case of the Python programming language, the initialization would look like this: weights=np.zeros((layer[l],layer[l-1]))
- Initialization with values of one: In this case, the initialization would look like this in the Python programming language: weights=np.ones((layer[l],layer[l-1]))
- Initialization using random values: In this case, if we take the case of the Python programming language, the initialization would look like this: weights=np.random.randn(layer[l],layer[l-1]) * 0.01
- Initialization using the He Initialization: In this case, the formula for initializing the weights would look like this: weights=np.random.randn(layer[l],layer[l-1])*np.sqrt(2/layer[l-1]).

For the initializations listed above, *layer* represents a python array that contains the dimensions for each layer in the neural network, and l represents the index of the current layer (on which layer we are).

We also mention other initialization methods such as the random uniform initialization (the values are taken from a uniform distribution), or the normalized Xavier weight initialization. In addition, in the case of initialization with zero, for example, it is possible to obtain an accuracy of 50%, while using the He initialization the accuracy can increase up to 95%.

9 Conclusion

The complexity of attacks, their impact on users, institutions, companies, or governments, and the methods used by hackers to create malware and implicitly, ransomware, evolve from day to day. Compared to classic, traditional methods, approaches that use machine learning or deep learning algorithms clearly have an advantage when we are faced with zero-day attacks, and the response time must be as short as possible. Also, the from-scratch implementations of algorithms based on machine learning or deep learning in favor of the use of already existing libraries offer a deep understanding of every aspect of the algorithm, better confidence for programmers, and an openness to develop and adapt an algorithm that works on a specific case in an algorithm that works in a much more general case.

References

[1] L. Y. Connolly, David S.Wall, Michael Lang, Bruce Oddson, *An empirical study of ransomware attacks on organizations: an assessment of severity and salient factors affecting vulnerability*, Journal of Cybersecurity, 2020

[2] Peter Eder-Neuhauser, Tanja Zseby, Joachim Fabini, *Malware propagation in smart grid networks: metrics, simulation, and comparison of three malware types*, Journal of Computer Virology and Hacking Techniques, 2019

[3] Nadeem Shah, Mohammed Farik, *Ransomware - Threats, Vulnerabilities And Recommendations*, International Journal of Scientific and Technology Research, 2017

[4] Mohammad Masum, Jobair Hossain Faruk, Hossain Shahriar, Kai Qian, Dan Lo, Muhaiminul Islam Adnan, *Ransomware Classification and Detection With Machine Learning Algorithms*, IEEE Annual Computing and Communication Workshop and Conference, 2022

[5] Urooj Umara, Bander Al-rimy, Zainal Anazida, Ghaleb Fuad, Rassam Murad, *Ransomware Detection Using the Dynamic Analysis and Machine Learning: A Survey and Research Directions*, Journal Applied Sciences, 2021.

[6] Malwarebytes Labs, *Top 5 ransomware detection techniques: Pros and cons of each*, October 2022

[7] Zahoora, U., Khan, A., Rajarajan, M. et al., *Ransomware detection using deep learning based unsupervised feature extraction and a cost-sensitive Pareto Ensemble classifier.*, Sci Rep 12, 15647 (2022). https://doi.org/10.1038/s41598-022-19443-7

[8] Fernando, D.W.; Komninos, N.; Chen, T., *A Study on the Evolution of Ransomware Detection Using Machine Learning and Deep Learning Techniques.* IoT 2020, 1, 551-604. https://doi.org/10.3390/iot1020030

[9] Mohammad Masum, Md Jobair Hossain Faruk, Hossain Shahriar, Kai Qian, Dan Lo, Muhaiminul Islam Adnan, *Ransomware Classification and Detection With Machine Learning Algorithms*, 2022

[10] S.H. Kok, Azween Abdullah, NZ Jhanjhi, *Early detection of crypto-ransomware using pre-encryption detection algorithm*, Journal of King Saud University - Computer and Information Sciences, Volume 34, Issue 5, 2022, Pages 1984-1999, ISSN 1319-1578, https://doi.org/10.1016/j.jksuci.2020.06.012.

[11] Masum, Mohammad, Hossain Faruk, Md Jobair Shahriar, Hossain Qian, Kai Lo, Dan Adnan, Muhaiminul, *Ransomware Classification and Detection With Machine Learning Algorithms.*, 10.1109,CCWC54503.2022.9720869, 2022.

[12] Akhtar, M.S.; Feng, T., *Detection of Malware by Deep Learning as CNN-LSTM Machine Learning Techniques in Real Time.*, Symmetry 2022, 14, 2308, https://doi.org/10.3390/sym14112308

[13] Li Chen, Chih-Yuan Yang, Anindya Paul, Ravi Sahita, *Towards resilient machine learning for ransomware detection*, 2019

[14] Singh Tanuvir, Di Troia Fabio, Visaggio Corrado Aaron, Austin Thomas,Stamp Mark. (2016). *Support vector machines and malware detection.* Journal of Computer Virology and Hacking Techniques. 12. 10.1007,s11416-015-0252-0.

[15] Abu Al-Haija, Q.; Odeh, A.; Qattous, H., *Malware Detection Based on Optimizable Decision Trees.*, Electronics 2022, 11, 3142.

[16] R. Ravula R., Chan C. and J. Liszka K., *DYNAMIC ANALYSIS OF MALWARE USING DECISION TREES.*,DOI: 10.5220/0003660200740083, In Proceedings of the International Conference on Knowledge Discovery and Information Retrieval (KDIR-2011), pages 74-83, ISBN: 978-989-8425-79-9

[17] Coin Desk, *Ransomware Payouts Declined in 2022: Crystal Blockchain*, https://www.coindesk.com/consensus-magazine/2022/12/22/ransomware-payouts-declined-in-2022-crystal-blockchain/

[18] The Washington Post, *Cyberattack on Maryland's health department was ransomware, officials say*, January 2022, https://www.washingtonpost.com/dc-md-va/2022/01/12/maryland-cyberattack-ransomware/

[19] Blackfog, *The State of Ransomware in 2022*, https://www.blackfog.com/the-state-of-ransomware-in-2022/

[20] Cybersecuty Insiders, *Conti Ransomware hits British Company KP Snacks*, https://www.cybersecurity-insiders.com/conti-ransomware-hits-british-company-kp-snacks/

[21] Bleeping Computer, *Cookware giant Meyer discloses cyberattack that impacted employees*, https://www.bleepingcomputer.com/news/security/cookware-giant-meyer-discloses-cyberattack-that-impacted-employees/

[22] TechMonitor, *Has DarkSide returned? Notorious ransomware gang may be behind German oil attack*, https://techmonitor.ai/technology/cybersecurity/german-oil-company-attack-blackcat

[23] PentaSecurity, *[Security Weekly] Airport Services Giant Swissport Struck by AlphV/BlackCat Ransomware*, https://www.pentasecurity.com/blog/security-weekly-swissport-alphv-blackcat-ransomware/

[24] Infosecurity Magazine, *Toyota Halts Production Across Japan After Ransomware Attack*, https://www.infosecurity-magazine.com/news/toyota-production-japan-ransomware/

[25] Arctic Wolf, *Top Cyber Attacks of March 2022*, https://arcticwolf.com/resources/blog/top-cyber-attacks-march-2022/

[26] IT Governance UK, *Coca-Cola Investigating Claims that a Ransomware Gang Stole Sensitive Data*, https://www.itgovernance.co.uk/blog/coca-cola-investigating-claims-that-a-ransomware-gang-stole-sensitive-data

[27] Security Boulevard, *Stormous Claims Credit for Ransomware Attack on Coca-Cola*, https://securityboulevard.com/2022/04/stormous-claims-credit-for-ransomware-attack-on-coca-cola/

[28] Ammar Odeh, Qasem Abu Al-Haija, Hazem Qattous, *PDF Malware Detection Based on Optimizable Decision Trees*, Electronics, 2022

[29] DataBreaches.net, *SCOOP: Glenn County Office of Education paid $400k ransom after ransomware attack*, https://www.databreaches.net/scoop-glenn-county-office-of-education-paid-400k-ransom-after-ransomware-attack/

[30] Cyber Management Alliance, *5 Major Ransomware Attacks of 2022*, https://www.cm-alliance.com/cybersecurity-blog/5-major-ransomware-attacks-of-2022

[31] Bleeping Computer, *Vice Society ransomware claims attack on Italian city of Palermo*,https://www.bleepingcomputer.com/news/security/vice-society-ransomware-claims-attack-on-italian-city-of-palermo/

[32] Y. Meidan, et al., *Detection of unauthorized IoT devices using machine learning techniques*, 2017, arXiv preprint arXiv:1709.04647

[33] Ban Mohammed Khammas, *Ransomware Detection using Random Forest Technique*,ICT Express, 2020, ISSN 2405-9595, https://doi.org/10.1016/j.icte.2020.11.001

[34] Security Magazine, *University of Pisa suffers ransomware attack*, https://www.securitymagazine.com/articles/97826-university-of-pisa-suffers-ransomware-attack

[35] Security Affairs, *French telephone operator La Poste Mobile suffered a ransomware attack*, https://securityaffairs.co/133080/cyber-crime/la-poste-mobile-ransomware.html

[36] Bleeping Computer, *Bandai Namco confirms hack after ALPHV ransomware data leak threat*, https://www.bleepingcomputer.com/news/security/bandai-namco-confirms-hack-after-alphv-ransomware-data-leak-threat/

[37] Tech Monitor, *LockBit ransomware gang claims attack on Italian tax office*, https://techmonitor.ai/technology/cybersecurity/italy-ransomware-lockbit-tax-office

[38] Bleeping Computer, *LockBit claims ransomware attack on Italian tax agency*, https://www.bleepingcomputer.com/news/security/lockbit-claims-ransomware-attack-on-italian-tax-agency/

[39] InfoSecurity Magazine, *Ransomware Group Demands £500,000 From School*, https://www.infosecurity-magazine.com/news/ransomware-group-500000-school/

[40] Bleeping Computer, *French hospital hit by $10M ransomware attack, sends patients elsewhere*, https://www.bleepingcomputer.com/news/security/french-hospital-hit-by-10m-ransomware-attack-sends-patients-elsewhere/

[41] Security Affairs, *France hospital Center Hospitalier Sud Francilien suffered ransomware attack*, https://securityaffairs.co/134771/cyber-crime/center-hospitalier-sud-francilien-ransomware.html

[42] Bleeping Computer, *Montenegro hit by ransomware attack, hackers demand $10 million* https://www.bleepingcomputer.com/news/security/montenegro-hit-by-ransomware-attack-hackers-demand-10-million/

[43] CyberThreat.Report, *Montenegro hit by ransomware attack, hackers demand $10 million*, https://www.cyberthreat.report/montenegro-hit-by-ransomware-attack-hackers-demand-10-million-update/

[44] Bleeping Computer, *Quantum ransomware attack disrupts govt agency in Dominican Republic*, https://www.bleepingcomputer.com/news/security/quantum-ransomware-attack-disrupts-govt-agency-in-dominican-republic/

[45] Cyber Management Alliance, *Recent Cyber Attacks Data Breaches Ransomware Attacks September 2022*, https://www.cm-alliance.com/cybersecurity-blog/recent-cyber-attacks-data-breaches-ransomware-attacks-september-2022Ransomware

[46] The guardian, *AFP investigates $1m ransom demand posted online for allegedly hacked Optus data*, https://www.theguardian.com/business/2022/sep/24/afp-investigates-1m-ransom-demand-posted-online-for-allegedly-hacked-optus-data

[47] Lee J, Jang H, Ha S, Yoon Y., *Android Malware Detection Using Machine Learning with Feature Selection Based on the Genetic Algorithm.*, Mathematics. 2021; 9(21):2813. https://doi.org/10.3390/math9212813

[48] Whitley, D., *A genetic algorithm tutorial.*, Stat. Comput. 1994, 4, 65–85.

[49] Malwarebytes, *Optus data breach "attacker" says sorry, it was a mistake*, https://www.malwarebytes.com/blog/news/2022/09/optus-data-breach-attacker-says-sorry-it-was-a-mistake

[50] The Denver Post, *Denver suburb won't cough up millions in ransomware attack that closed city hall*, https://www.denverpost.com/2022/09/22/wheat-ridge-ransomware-fremont-county-cyber-attack/

[51] Databreaches.net, *Scoop: Tift Regional Medical Center victim of ransomware attack in July*, https://www.databreaches.net/scoop-tift-regional-medical-center-victim-of-ransom-attack-in-july/

[52] Zhang Zonghua, Yan Jinpei, Qi Yong, Rao Qifan, *Detecting Malware with an Ensemble Method Based on Deep Neural Network*, Security and Communication Networks, 2018, https://doi.org/10.1155/2018/7247095

[53] Nanda Rani, Sunita Vikrant Dhavale, *Leveraging Machine Learning for Ransomware Detection*, 2022

[54] CyberNews, *UK car dealer Pendragon hit with a record ransom demand*, https://cybernews.com/news/pendragon-record-ransom-demand/?utm$_{s}ource = linkedinutm_{m}edium = socialutm_{c}ampaign = cybernewsutm_{c}ontent = post$

[55] Bleeping Computer, *Pendragon car dealer refuses \$60 million LockBit ransomware demand*, https://www.bleepingcomputer.com/news/security/pendragon-car-dealer-refuses-60-million-lockbit-ransomware-demand/

[56] CryptoPotato, *Brazil's BRB Bank Pays 50 BTC After Being Targeted by a Ransomware Attack*, https://cryptopotato.com/brazils-brb-bank-pays-50btc-after-being-targeted-by-a-ransomware-attack/

[57] Inside Bitcoin, *Bank of Brasilia to pay 50 BTC after a ransomware attack*, https://insidebitcoins.com/news/bank-of-brasilia-to-pay-50-btc-after-a-ransomware-attack

[58] The Record, *French defense firm denies ransomware attack after leak site posting*, https://therecord.media/french-defense-firm-denies-ransomware-attack-after-leak-site-posting/

[59] Bleeping Computer, *LockBit ransomware claims attack on Continental automotive giant*, https://www.bleepingcomputer.com/news/security/lockbit-ransomware-claims-attack-on-continental-automotive-giant/

[60] Techmonitor, *FBI joins investigation into Continental ransomware attack*, https://techmonitor.ai/technology/cybersecurity/continental-cyberattack-ransomware-lockbit-fbi

[61] Security Affairs, *LockBit 3.0 gang claims to have stolen data from Kearney Company*, https://securityaffairs.co/138136/cyber-crime/lockbit-ransomware-kearney-company.html

[62] SC Media, *Intrado ransomware attack claimed by Royal ransomware gang*, https://www.scmagazine.com/brief/ransomware/intrado-ransomware-attack-claimed-by-royal-ransomware-gang

[63] Bleeping Computer, *Royal ransomware claims attack on Intrado telecom provider*, https://www.bleepingcomputer.com/news/security/royal-ransomware-claims-attack-on-intrado-telecom-provider/

[64] Data Breach Today, *LockBit Group Claims Attack on Port of Lisbon*, https://www.databreachtoday.com/lockbit-group-claims-attack-on-port-lisbon-a-20830?highlight=true

[65] Bleeping Computer, *LockBit ransomware claims attack on Port of Lisbon in Portugal*, https://www.bleepingcomputer.com/news/security/lockbit-ransomware-claims-attack-on-port-of-lisbon-in-portugal/

[66] Machine Learning Mastery, *Why Initialize a Neural Network with Random Weights?*, https://machinelearningmastery.com/why-initialize-a-neural-network-with-random-weights/

[67] Machine Learning Mastery, *Weight Initialization for Deep Learning Neural Networks* , https://machinelearningmastery.com/weight-initialization-for-deep-learning-neural-networks/

[68] Towards Data Science, *Why better weight initialization is important in neural networks?*, https://towardsdatascience.com/why-better-weight-initialization-is-important-in-neural-networks-ff9acf01026d

[69] Towards Data Science, *Random Initialization For Neural Networks: A Thing Of The Past*, https://towardsdatascience.com/random-initialization-for-neural-networks-a-thing-of-the-past-bfcdd806bf9e

[70] Baeldung, *Random Initialization of Weights in a Neural Network*, https://www.baeldung.com/cs/ml-neural-network-weights

[71] Deepchecks, *Neural networks and random initialization.* https://deepchecks.com/glossary/random-initialization/

[72] Machine Learning Mastery, *Benefits of Implementing Machine Learning Algorithms From Scratch*, https://machinelearningmastery.com/benefits-of-implementing-machine-learning-algorithms-from-scratch/

[73] Towards Data Science, *Parameters and Hyperparameters in Machine Learning and Deep Learning*, https://towardsdatascience.com/parameters-and-hyperparameters-aa609601a9ac

[74] Eder-Neuhauser, P., Zseby, T., Fabini, J., *Malware propagation in smart grid networks: metrics, simulation and comparison of three malware types.*, J Comput Virol Hack Tech 15, 109–125 (2019). https://doi.org/10.1007/s11416-018-0325-y

[75] Lena Yuryna Connolly, David S Wall, Michael Lang, Bruce Oddson, *An empirical study of ransomware attacks on organizations: an assessment of severity and salient factors affecting vulnerability*, Journal of Cybersecurity, Volume 6, Issue 1, 2020, tyaa023, https://doi.org/10.1093/cybsec/tyaa023

[76] Shah Nadeem, Farik Mohammed, *Ransomware-Threats, Vulnerabilities And Recommendations.*, 2017 International Journal of Scientific and Technology Research. 6. 307-309.

[77] Giyoon Kim, Soram Kim, Soojin Kang, Jongsung Kim, *A Method for Decrypting Data Infected with Hive Ransomware*, 2022

[78] Alqahtani, Abdullah, and Frederick T. Sheldon. 2022, *A Survey of Crypto Ransomware Attack Detection Methodologies: An Evolving Outlook*, Sensors 22, no. 5: 1837, https://doi.org/10.3390/s22051837

[79] Zahoora, U., Khan, A., Rajarajan, M. et al., *Ransomware detection using deep learning based unsupervised feature extraction and a cost sensitive Pareto Ensemble classifier*, Sci Rep 12, 15647, 2022, https://doi.org/10.1038/s41598-022-19443-7

[80] CYDERS, *State of Ransomware 2022*, 2022

[81] IBM Security, *Definitive guide to ransomware 2022*, 2022

[82] Ekta Gandotra, Divya Bansal, Sanjeev Sofat, *Malware Analysis and Classification: A Survey*, 2014