Literature Review

Benjamin Lee Xin Lone

registration: 100292465

1 Abstract

This paper will look into the possibility of using machine learning to identify and combat malware/ransomware.

2 Introduction

In today's world, more than 47.4% of the worlds households own computers (Thomas, 2019). In addition, the pandemic has mad a proportion of the world's populace to work from home, increasing computer sales by 13% in comparison to the year before (Carly, 2021). According to the IC^3 report there has been a 69% increase in cybercrime rates compared to the previous year (Cyber Crime Report, 2020). Of the many different types of cybercrimes, one of the most common types is the use of malware and worms, which infects a computer to gather the users information without their permission. Ransomware is type of malware that spreads easily, using web URLs as well as email attachments, the malware will apply a kind of lock on the users files using encryption that can only be unlock using the generated key held by the actor with the only way to unlock it being to pay a ransom.

3 Malware

3.1 Ransomware

Dating back to the 1980's, ransomware is an infectious malware that encrypts important data on the users computer preventing them from accessing certain files or in some cases their entire computer, with the only means of recovering them being to pay the ransom. The first ever known use of such malicious tactics dated back to 1989, where floppy disks were used to spread **PC CYBORG / AIDS Trojan**, this particular ransomware once installed would replace the *autoexec.bat* causing the computer to perform multiple reboots before requesting the user to pay a ransom of $378 (Babu and Nittin, 2010). Over the years, ransomware has since evolved to make it work together with information stealing malware, targeting individuals important files and locking them up with an encryption. Ransomware is especially dangerous with the existence of the internet connecting everything together, making it easier to spread.

3.1.1 How ransomware works

In many cases, ransomware is a malware or software that locks users out of important files and documents, most of the time demanding a ransom to be paid. The way they lock the users out is through the use of encryptions that can only be unencrypted by a special key, which is generated after the encryption process of the device is completed. This category of ransomware are the most common, and they are usually referred to as crypto ransomware (Scaife et al., 2016).

Alongside crypto ransomware are locker and hybrid ransomware. locker ransomware prevents the user from accessing their devices entirely, sometimes even demanding for the ransom to be paid trough IoT devices that were originally connected to the targeted device (Yaqoob et al., 2017). Hybrid Ransomware is the most dangerous but also the most rarest of the three can launch an attack from the front-end but also back-end of any IoT devices (Yaqoob et al., 2017). This makes it very difficult for the user to even salvage the device entirely, with the files not only being encrypted but the entire computer being locked out from reinstalling the operating system.

Once infected, the ransomware will look through files, mostly documents, images, but sometimes also zip files as they may contain important information. This is done in order to save time, as the owner of the original files would find documents and images more important than random applications (Gazet, 2010). The ransomware would than proceed to select files that it would see as important and encrypt them before finally displaying the ransom message.

3.2 Currently known ransomware

3.2.1 WannaCry(2017)

WannaCry was one of the most widespread ransomware to have existed, it mainly targeted large companies. Unlike other type of ransomware's, WannaCry would encrypt **all** the data in the system, leaving 2 files that tells the user to pay a ransom (Savita and Manisha, 2017).

WannaCry was special in the way it infects computers, it works more like a worm than it would a malware. The initial program would first be activated, where it will then search through the computers in the shared network installing the ransomware replacing an application found in older versions of windows called taskche.exe. This will then start the encryption process starting from the windows registry, where it will install autorun programs as well as processes that support and protect the ransomware program (Kao and Hsiao, 2018).

3.2.2 CryptoLocker

Cryptolocker is another variant of crypto ransomware, the malware which is originally a zip file disguises itself as a pdf documents. CryptoLocker locks important files, including the likes of Photoshop files, PDF and any files coming from the Microsoft Office Family of products (Hansberry et al., 2014). CryptoLocker uses an AES key to encrypt the user files, storing the key in a remote server until the ransom is paid.

3.3 A look at current countermeasures

3.3.1 Cuckoo (Analysis Software)

Cuckoo is a software used to identify malware samples and test's them in a enclosed virtual machine. The software also tests the actions of the malware, learning how it works and how it behaves before producing a report (Chen and Bridges, 2017).

3.3.2 Unveil (Analysis Software)

Unveil uses a dynamic analysis system to detect threats while recreating how the ransomware acts. Unlike cuckoo, unveil is uses dissimilarity score of desktops screenshots before, during and after executing the malware. This allows unveil to collect data on any new ransomware variants through the use of real time desktop analysis, this method has already been successful in identifying previously evasive variants and has created countermeasures against them (Chen and Bridges, 2017).

3.3.3 Backup SSDs

NAND flash based SSDs contain backup mechanisms which works even if the machine did indeed get infected by ransomware. This is due to how the mechanism works, which keeps previous versions of backup data until the internal Garbage Collection process starts(Min et al., 2018). The special mechanism in NAND SSDs are what makes them especially good against the threat of ransomware, in comparison to normal SSDs that erases data's in blocks, while NAND SSD's writes the data in blank pages to while waiting for the Garbage Collection process to commence.

3.4 Machine Learning

Machine learning has provided computers with a way to improve through gaining experience, with the help of algorithms and data sets, computers can now adapt to situations in real time without the need for sophisticated hardware. In order for machine learning to be accurate, a candidate program which is produced using various algorithms and functions, is tested based on the accuracy of its decisions (Jordan and Mitchell, 2015). Each candidate programs accuracy will be tested depending on the task they would be required to do.

3.4.1 Against dynamic malware

There are various academic works that have been published over the years regarding the use of machine learning techniques on malware. Schultz et al. (2001) suggested the use of data mining, to find patterns in large quantities of data and using them to detect future occurrences. A comparison was then made between the malware detection system using the data mining method and a cross-validation system that checked the executable files certificate. The data mining method won with a 97.76% detection rate which was double of what the cross-validation method was able to produce. A newer study suggests a combination of data mining method, dynamic behaviour monitoring and classification techniques to effectively detect malware (Firdausi et al., 2010).

When combating a threat that can produces new instances of itself, there are several questions that must be taken into consideration. When categorising malware that has not been identified before, does it belong to an existing family of malware, what makes it different from others and what malware family does its behaviour resembles the most (Rieck et al., 2008). This will be important when categorising unknown malware variables for future use, making it easier for the program to identify.

Evasive malware is a dynamic malware that camouflages its behaviour in order to avoid detection, with the only way to identify it through a bare-metal environment (Kirat and Vigna, 2015). This process allows the malware to be run on a virtual system where it will be clearer to see the processes taking place.

3.4.2 Against dormant malware

Dormant malware are more trickier to identify then their dynamic/active counterparts. This is due to their ability avoid the various dynamic malware detection techniques, as those tools are only capable of detecting malware through behaviour. A paper produced by Comparetti et al. (2010) suggests exploiting the shared code found in a majority of malware. The author of the paper did this by using a Re animator, a novel approach that identifies dormant behaviours in the malware binaries. This can work well together with a technique used in identifying malware on android devices called one-class support vector machine, where if there is a code that is similar to a previously identified malware, it would get rid of it immediately (Sahs and Khan, 2012).

3.5 How data on malware is gathered

3.5.1 Honeypots

A Honeypot is a term used for computers that are voluntarily vulnerable to malware for the sole purpose of studying its behaviour (Santos et al., 2013). This method however will create a large volume of collected traffic due to the amount of large files being transferred to the monitoring device. The large amount of complex data also makes it difficult for humans to analyse it manually, leading to many instances where machine learning is called upon.

3.6 Datasets for machine learning

A malware dataset containing the data on malware API calls is available on github which can be used to combat dynamic malware. On the same page, a dataset containing the classification of metamorphic malware is also included. Both datasets contains the executables and behaviours from previous generations of malware, the data is complied into a csv file using cuckoo(Catak et al., 2021).

3.6.1 Disadvantages of using machine learning

Machine learning has indeed been depended upon by many malware detection tools, however because of this many attackers are creating malware that can evade getting detected by machine learning algorithms. Recent studies have found machine learning systems can be evaded algorithmically or with the use of other machine learning models (Anderson et al., 2017).

3.7 Hardware base malware detection

3.7.1 Use of temperature

There have been instances where temperature was used to detect malware. This method is said to be especially effective on mobile phones or devices where temperatures rapidly increase according to the amount of active activities. This is because heavy resource task require more power which in turn increases battery consumption and the temperature of at which the battery produces. Temperature however is only effective when it is used to identify active malware, when it uses hardware resources such as CPU, memories and batteries (Kurniawan et al., 2015). Using temperature to detect malware can be effective on computers is the right components to monitor are selected. A survey conducted by Larsen et al. (2021) suggest that CPU temperature, loads and clock speed were the three most influential in regards to detecting malware.

3.7.2 Use of computer physical sensors

A study produced by Michael et al. (2017), suggests the use of the sensors embedded into computer components to detect ransomware. A majority of modern computers have sensors built into their hardware components which supply information for the various subsystems within the computer. The sensor system is a very important component to any computer as it help correct internal environment if the readings were to be abnormal. Computer components are made up of transistors that features sizing on a nanometre scale. This will result in the computer relying on a large number of transistors to correspond with the systems activity resulting increasing the power consumption and the amount of heat the computer produces. This allows us to find out which component is being used at a specific time during a heavily resource task such as encryption. Embedded sensors can be used in order to detect this instances, monitoring computer activity using temperature, power and battery voltage. By monitoring the data of the embedded sensors in specified times, one could identify when resource heavy task such as a malware attack may be occurring. Every small yet distinguishable change in the computers hardware will be reported by the on-board sensor, this would make working with a single section of the machine redundant. Instead of focusing on a single aspect of the machine, increasing the amount of sensors being monitored using a feature vector will allow the machine to classify the physical state in much more detail, allowing us to see the specific tasks being completed and the sequence at which the malware/ransomware is.

3.7.3 Malware detection through monitoring power consumption

Another study monitored the power consumption and network resources of both a non-affected and an affected computer. The power consumption of computers is dependent on the software that is being used, which means that heavily resource process such as an encryption would use up more power then normal uses. The data was collected using the DAQ for power consumption and wireshark for the network traffic data (Hernandez Jimenez and Goseva-Popstojanova, 2019). Two sets of data will be provided for the machine learning program, a data set where normal applications were run and the other with malware. To benchmark and collect data, the computer was left to idle for three minutes using a clean version of windows running non malicious apps and another version of windows with the malware installed. This was repeated multiple times, the results showed that the power-only based detection provided the better protection over a network only based one, with a combination of the two providing the best protection overall (Hernandez Jimenez and Goseva-Popstojanova, 2019).

3.7.4 Use of HPC to detect malware activity

HPC or hardware performance counter-based are a set of special registers that are built into microprocessors performance monitoring unit and is used to store hardware-related activities. HPC provide access to detailed performance information with much lower overheads in comparison to their software counterparts(Kirat and Vigna, 2015). This can be used together with a linux based application called Perf which analyses performance and traces data, the special feature embedded into this program is the ability to view specific hardware events on per process and per CPU basis. The HPC based detection and identification process usually takes two steps, logging HPC events and then performing the analysis of that data. This process however would significant strain on the monitored devices storage overhead, due to the amount of HPC profiles each storing data on clean software modules and existing malware. This method will allow us to detect malware based on hardware performance analysis while also tracing the various processes causing issues through the use of Perf.

3.8 A conclusion on the literature review

From this literature review we can conclude the use of software based malware detection to be unsustainable, as bad actors find new ways to prevent detection. Implementing hardware based malware detection will provide an additional layer of security by providing details of certain changes in the hardware systems. Monitoring physical components such as CPUs and hard-drives, can allow us to monitor for malware attacks by detecting minor changes in temperature, clock-speed, transfer speed, etc. Using hardware based detection would also prevent camouflage malware and dormant malware from stalling their attack, as there won't be any software based detection systems to evade.

References

Anderson, H., Kharkar, A., Filar, B., and Roth, P. (2017). Evading machine learning malware detection.

Babu, N. G. and Nittin, J. (2010). The emergence of ransomware.

Carly, P. (2021). Pc sales just broke a 10-year record thanks to the pandemic.

Catak, F. O., Ahmed, J., Sahinbas, K., and Khand, Z. H. (2021). Data augmentation based malware detection using convolutional neural networks. *PeerJ Computer Science*, 7:e346.

Chen, Q. and Bridges, R. A. (2017). Automated behavioral analysis of malware: A case study of wannacry ransomware. In *2017 16th IEEE International Conference on Machine Learning and Applications (ICMLA)*, pages 454–460.

Comparetti, P. M., Salvaneschi, G., Kirda, E., Kolbitsch, C., Kruegel, C., and Zanero, S. (2010). Identifying dormant functionality in malware programs. In *2010 IEEE Symposium on Security and Privacy*, pages 61–76.

Cyber Crime Report (2020). Internet crime report 2020.

Firdausi, I., lim, C., Erwin, A., and Nugroho, A. S. (2010). Analysis of machine learning techniques used in behavior-based malware detection. In *2010 Second International Conference on Advances in Computing, Control, and Telecommunication Technologies*, pages 201–203.

Gazet, A. (2010). Comparative analysis of various ransomware virii.

Hansberry, A., Lasser, A., and Tarrh, A. (2014). Cryptolocker: 2013's most malicious malware.

Hernandez Jimenez, J. and Goseva-Popstojanova, K. (2019). Malware detection using power consumption and network traffic data. In *2019 2nd International Conference on Data Intelligence and Security (ICDIS)*, pages 53–59.

Jordan, M. I. and Mitchell, T. M. (2015). Machine learning: Trends, perspectives, and prospects. *Science*, 349(6245):255–260.

Kao, D.-Y. and Hsiao, S.-C. (2018). The dynamic analysis of wannacry ransomware. In *2018 20th International Conference on Advanced Communication Technology (ICACT)*, pages 159–166.

Kirat, D. and Vigna, G. (2015). Malgene: Automatic extraction of malware analysis evasion signature. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, CCS '15, page 769–780, New York, NY, USA. Association for Computing Machinery.

Kurniawan, H., Rosmansyah, Y., and Dabarsyah, B. (2015). Android anomaly detection system using machine learning classification. In *2015 International Conference on Electrical Engineering and Informatics (ICEEI)*, pages 288–293.

Larsen, E., Noever, D., and MacVittie, K. (2021). A survey of machine learning algorithms for detecting ransomware encryption activity.

Michael, T., Kaitlin, S., and Mitchell, T. (2017). Sensor-based ransomware detection. In *Future Technologies Conference (FTC) 2017*, volume 29-30 November 2017.

Min, D., Park, D., Ahn, J., Walker, R., Lee, J., Park, S., and Kim, Y. (2018). Amoeba: An autonomous backup and recovery ssd for ransomware attack defense. *IEEE Computer Architecture Letters*, 17(2):245–248.

Rieck, K., Holz, T., Willems, C., Düssel, P., and Laskov, P. (2008). Learning and classification of malware behavior. In Zamboni, D., editor, *Detection of Intrusions and Malware, and Vulnerability Assessment*, pages 108–125, Berlin, Heidelberg. Springer Berlin Heidelberg.

Sahs, J. and Khan, L. (2012). A machine learning approach to android malware detection. In *2012 European Intelligence and Security Informatics Conference*, pages 141–147.

Santos, I., Devesa, J., Brezo, F., Nieves, J., and Bringas, P. G. (2013). Opem: A static-dynamic approach for machine-learning-based malware detection. In Herrero, Á., Snášel, V., Abraham, A., Zelinka, I., Baruque, B., Quintián, H., Calvo, J. L., Sedano, J., and Corchado, E., editors, *International Joint Conference CISIS'12-ICEUTE 12 Special Sessions*, pages 271–280, Berlin, Heidelberg. Springer Berlin Heidelberg.

Savita, M. and Manisha, P. (2017). A brief study of wannacry threat: Ransomware attack 2017. Volume 8, No. 5, May-June 2017.

Scaife, N., Carter, H., Traynor, P., and Butler, K. R. B. (2016). Cryptolock (and drop it): Stopping ransomware attacks on user data. In *2016 IEEE 36th International Conference on Distributed Computing Systems (ICDCS)*, pages 303–312.

Schultz, M., Eskin, E., Zadok, F., and Stolfo, S. (2001). Data mining methods for detection of new malicious executables. In *Proceedings 2001 IEEE Symposium on Security and Privacy. S P 2001*, pages 38–49.

Thomas, A. (2019). Share of households with a computer at home worldwide from 2005 to 2019.

Yaqoob, I., Ahmed, E., ur Rehman, M. H., Ahmed, A. I. A., Al-garadi, M. A., Imran, M., and Guizani, M. (2017). The rise of ransomware and emerging security challenges in the internet of things. *Computer Networks*, 129:444–458. Special Issue on 5G Wireless Networks for IoT and Body Sensors.