A Critical Review Of File-Less Malware, Attacks And Detection Techniques For Mitigating Them

[1] Obini, U. C., [2] Onu, F. U., [3]Ede, M. O., [4]Okorie, K. M.,
[5]Igwe, J. S., [6]Egbono, F.

[1,2,5]Department of Computer Science, Ebonyi State University, Abakaliki– Nigeria.
[3]Department of Computer Science, Coal City University, Enugu– Nigeria.
[4]ICT Department, Eagle Hauleage, Lagos– Nigeria.
[6]Department of Software Engineering, University of PortHarcourt– Nigeria.

Abstract

This paper presented a critical study of file-less malware attacks and the detection techniques for mitigating these attacks on computer systems or software platforms. The study started by presenting an overview of file-less malwares, types of the file-less malwares that can be encountered and various techniques adopted in detecting and tackling the challenges posed by file-less malwares. The work studied signature-based technique, behavior-based technique, heuristic methods, IoT-based methods and machine learning methods. Further in the work, we introduced adversarial machine learning technique and how attackers implement this technique for the development of intelligent malware that is capable of maneuvering other detection techniques. In this work, the application of machine learning (deep neural network) has been presented as the most effective means that can be applied for an effective detection of file-less malware of any type. Consequently, the study recommended that future research works should aim at adopting deep learning techniques for the mitigation of adversarial and in fact all types of file-less malware attacks.

***Keywords**: File-less Malware, Machine Learning, LOLBins, LOLScripts, Adversarial Perturbation*

Date of Submission: 22-07-2023 Date of Acceptance: 02-08-2023

I. INTRODUCTION

The computer system (hardware and software) has historically experienced a lot of malicious attacks on a constant basis. The attacks are multi-faceted and of various types. [1] Listed the top 20 most common cyber-attacks to include those shown in figure 1.

Among all these attacks, Malicious Software (malware) is very dangerous because they can mutate themselves. The development of these malware programs occur when programmers create software which is harmful to the files on a computer system and the computer system itself in such a way that no anti-virus program will be able to recognize or detect its presence in the system. The whole threat landscape was changed in 2022 by the development of the file-less malware in the industry. This type of malware is capable of staying on the computer system, making changes to the computer and the file system without being detected [2][3].

The conventional malware attacks make use of real malicious software executable. The file-less malwares operates on the system by attack and hide by leveraging on trusted legitimate processes like Living Off the Land Binaries (LOLBins), Living Off the Lang Binaries and Scripts [4] and other built-in tools. These malware attacks do not download malicious files to the system or write contents on the memory disk in order to compromise the system. The attacks by exploiting almost the vulnerable application to inject codes that are malicious into the system main memory [5].

i. Denial-of-service (DoS) and distributed denial-of-service (DDoS)
ii. Man-in-the-middle (MITM)
iii. Phishing
iv. Whale-phishing
v. Spear-phishing
vi. Ransomware
vii. Password
viii. Structured Query Language (SQL) Injection
ix. URL Interpretation
x. Domain Name System (DNS) Spoofing
xi. Session Hijacking
xii. Brute force
xiii. Web
xiv. Insider Threats
xv. Trojan Horses
xvi. Drive-by
xvii. cross-site scripting (XSS)
xviii. Eavesdropping
xix. Birthday
xx. Malware

Figure 1: List of top 20 common cyber-attacks [1]

Machine learning has provided great success in solving pattern recognition problems and has gained increased application in cyber security. However, hackers today employed adversarial perturbation approach to develop cyber-attack models which are dynamic and often appear invisible to the conventional machine learning based security solutions, and hence, attack the target network infrastructure without much resistance. This has remained a very big problem all over the world and therefore requires urgent solution. The benefit of solving this problem will restore system reliability, integrity and data confidentiality over the network among other advantages

This work will benefit all industrial stakeholders both in the public and private sectors like the network administrators, cloud managers, IT security consultant, government and military agencies for the security of classified data, and even the common man. This system will ensure the protection of their internet of things against cyber-attack.

II. OVERVIEW OF FILE-LESS MALWARE

The problems of malware on computers are common problems various kinds of organization over the world encounter. It does not always appear normally like other infections known to humans and other living things. It is usually being created by developers [6]. The good news is that researchers have been making enough efforts to mitigate the thriving force of these viruses and if possible, bring it to a drastic end. Some preventive measures that have been good over the years is the development of ant-virus software, which regularly scans the computer system and eliminate various form of threats encountered. However, a non-malware attacked was created and distributed into computer systems [3]. This type of virus always has a way of staying hidden and not being detected during scans by the antivirus because there's no executable file associated with it and it resides on the main memory of the system and subsequently make changes to file systems [7].

There are various vulnerabilities associated with system attacks that use file-less malware technique. The vulnerabilities are as a result of installed applications to the system which could be web browsers, MS office, PDF viewers, etc. Whenever any of the vulnerabilities are identified in the suspected application, scripts are loaded into running memory which is done without a physical touch on the file system [8][9]. This will give the attackers the access and capacity to control the system from anywhere they are.

[10] presented that "A new genus of malware has emerged that breaks the rules of traditional detection and defence methods, unlike other breeds of malware that require the installation of software on a victim's machine, file-less malware infects a host computer dynamic memory". File-less malware also has the ability to hijack Windows primarily making the power of the Operating System (OS) against the users with the use of common tools like PowerShell (which comes integrated into the Windows 8) to perform its malicious activities" [8].

According to [10], the steps that malwares take to attack are identified which begins with "…a fishing email, a visit to a malicious website, or the use of an infected USB flash memory stick, file-less malware scans the machine looking for vulnerabilities-whether it's unpatched Flash or a Java plug-in, or almost any process that involves PowerShell" they also went ahead to say that "Malicious websites may also download Flash or Java onto a user's machine. The payload then begins executing attack by using the dynamic memory of user's computer such as leveraging browsers processes" [10][11].

One thing about the file-less malware is that it remains persistent when launching an attack. It also has the capacity to reside within the OS for as much as months while propagating an attack without being noticed. According to [9] persistence is one the special area where such Tactics, Techniques, and Procedures (TTP) are exercise greater impact. Furthermore, hackers also use a very dark PowerShell infrastructure to drop a file-less malware on targeted computers, which as a result turns into fetched payloads from a command-and-control server [12].

III. TYPES OF FILE-LESS MALWARES

According to [5], "There are three categories of file-less malware, which are Memory Resident Malware (MRM), Window Registry Malware (WRM) and Rootkit files malware as discussed below;

Memory Resident File-less Malware (MRM)

([5][13] defined memory resident malware as the malware that occupies the main memory of the system without any contact with the file systems. The process it uses to possess and authenticate is usually legitimate to windows file in order to execute and stay there until it is triggered. The various types of memory resident file-less malware are:

1. **Code Red**: Code red basically infects Microsoft Internet Information Server (IIS) of version 4.0 and 5.0 having known the vulnerabilities of the buffer overflow. The system is infected with server GET/default.ida request on TCP port 8.0 allowing the worm to run the code on the server"[14] [15]
2. **SQL Slammer:** SQL slammer is a computer worm that is capable of choking the bandwidth of a network which in turn results to denial-of-service condition. The worm has applied the method to control and infect by performing a scan on the vulnerability of buffer over-flow on the internet [16].
3. **Lurk Trojan:**Lurk Trojan is a banking infection which is capable of either using the using command "regsrv32" and "netsh add helper dll (dynamic link library)" or via shell icon overlay identifiers branch of the system registry. The Trojan uses its features to gain access to the sensitive data of the user, and it can as well attack and compromise the user's online banking services and information [17].
4. **Poweliks:** Poweliks is a file-less malware that is originated from a conventional file-based malware known as wow-liks. The malware usually installs itself into the registry of the system and as equally use it to persist on attacking the system which results to its escape from antivirus software solutions since it did not leave any file written on the disk. Also, the malware runs an installation of PowerShell in the background without sending an alert to the defensive system if it is not already in the system. It was also noted that, "System is penetrated by exploiting the Microsoft office vulnerabilities and use PowerShell along with JavaScript with shell code" [18].

Windows Registry Malware

According to [4], "Registry is the database for storing low-level settings of the Operating System and some critical apps. In there, malware authors managed to store a complete malicious code into the registry in an encrypted manner. It makes it undetected" It was also identified that "For malware to remain persistence, it can exploit some operating system thumbnail cache using registry. The file is set to destroy itself once it carries out its malicious task [19][20].

Rootkit File-less Malware

This type of file-less malware gets the privileges of the administrators' level in order to hide the malicious code into the kernel of the Windows Operating System. [5][19][21], "The attacker can install this kind of malware after getting administrators level privilege to hide malicious code into the windows operating system. While this is not 100% file-less infection either, it fits here"

[6] Presented a study on the analysis of machine learning techniques for the detection of online malware in the cloud. The study adopted CNN, SVM, RF, K-NN, Gradient Boosted Classifier (GBC) and Gaussian Naive Bayes (GNB) respectively to solve the problem of malware on cloud architecture. The result showed that the CNN achieved the best performance with 92.9% accuracy compared to the SVM with 87.56%; RF with 89.36%; K-NN with 72.34%; GBC with 81.47% and GBN with 58.09%. Although the study has a nice performance accuracy for detection of malware in the cloud platform, However the study presented by [22] which proposed a malicious pdf detection model which can be applied for against the adversarial attack built from Benign pdf container JavaScript, shows that their still room for improvement for detection of adversarial attacks.

[23] Presented an integrated malware detection and classification system. The study argues that the increase of shadow internet economy has resulted to malware threats to computers and information system all over the world. The signature-based solution to these threats is not effective to unknown malware features and hence not reliable. New classification approaches based on static and dynamic methods all have their advantages and disadvantages; however, the use of dynamic detection techniques provided the best solution compared to the rest, but only very effective at the early stage of the attack. The study used a hybrid solution to solve the problem of malware detection and achieved accuracy of 97%; however, the algorithms never considered perturbated malware features. However, the study presented by [24] on adversarial malware detection lessons from pdf-based attacks, shows that it is necessary to engage a machine learning technique for the more accurate detection of malwares and adversarial attacks on computer systems.

[25] Presented a machine learning based malware detection solution using texture malware perturbation method. The aim of the study was to show that the present-day machine learning based solutions are vulnerable. To achieve this, perturbation features are added to the test dataset based on gradient descent and L-norm optimization method to attack networks. The result showed that the machine learning algorithms (RF, CNN, and SVM) achieved detection accuracy of 0% and 74.1% throughput to the attack. This means that the system completely lacks the ability to detect an adversarial perturbation malware attack. However, [26] presented a survey on adversarial attacks and defenses in malware classifications, which recommends that the further studies on malware detection and classification should consider adversarial attacks which is more intelligent than the conventional malwares and more harmful to the computer system.

[27] Presented research on malware classification based on probability scoring and machine learning technique. The study developed a solution which used probability threshold and spatial pyramid pooling-based CNN to develop a solution which can detect malware attack. The algorithm was trained with 174,607 samples of malware data from 63 classes of malware. The result achieved is 98.82% accuracy. However, the algorithms never considered perturbated malware features. However, this research work did not consider adversarial attacks, the survey by [28] on adversarial attacks for malware analysis, shows that the new form of attack that the computer system deserves more attention to defeat its intelligence using machine learning technique. Hence, despite the success there is still room for improvements.

[29] Compared various deep learning and shallow learning techniques for application programming interface calls malware prediction. The study used two datasets to compare various machine learning algorithm such as RF, XGboost, Extra trees, NODE, TabNet and their ability to detect malware. Their performances were evaluated with Receiver Operator Curve (ROC) and RF achieved the best ROC with 0.8094 via the call sequence dataset at a delay training time of 1284419ms. Meanwhile [30] presented a study on robust malware detection models which is focused on learning from adversarial attacks and defenses. This study presents the necessity of improving the defense mechanisms adopted for the protection of computer systems using machine learning techniques against dangerous attacks like adversarial attacks.

IV. FILE-LESS MALWARE DETECTION TECHNIQUES

In recent years the studies on malware detection have increased and the detection techniques in past are classified as signature-based detection and the behaviour-based detection. The classification encompasses various techniques such as heuristics base, data mining, model checking, internet of things, machine learning and deep learning

Signature-based detection

The most used and popular method for malware detection is pattern matching and signature-based detection. Each file is made up of distinct and unique feature which can be identified as the signatures, these features could be like fingerprint of an executable file. This signature-based detection technique uses the features and patterns recognized from previous malware attacks to identify them when there is an attempt to attack the system again. This method is a very quick and the fastest malware detection method. This is so because this method operates with special sensitivity because of their unique nature. They operate with a very low error rate and the small error rate is the major reason why this technique is often used on common commercial anti viruses [31][32].

However, this technique lacks the ability to detect and identify malwares that are unknown to them. In such cases, it requires a high amount of time, manpower and money to identify and extract the new unique signatures. These constraints are the major disadvantages of applying this particular technique. Another major challenge is its inability to confront against malwares that mutates their infection codes such as metamorphic and polymorphic codes. In order to handle these constraints, there are other malware detection techniques that were proposed by researchers. Even though they may not be effective at detecting unknown of polymorphic malwares easily, they have their own advantages as well [31].

Behaviour-based detection

This technique for malware detection carefully monitors and study the behaviors and characteristics of the program to identify whether is malicious or not. Due to this pattern of operation, this technique is not without limitations and cannot be expressed as a superior to the signature-based method since it is focused on the behavior of the program instead of what it says [33]. In these methods, programs with the same behaviour are collected. Thus, a single behaviour signature can identify various samples of malware. These types of detection mechanisms help in detecting malware that keep on generating new mutants since they will always use the system resources and services in the similar manner [8].

Heuristic Based Detection Technique

In the heuristic method detectors, the features acquired from the signature and behaviour techniques are combined in order to detect malwares and changes on the system depending on the activities that have occurred. Features like API calls, Opcode, CFG, list of DLLs, n-gram and other hybrid features are used for this operation [31]. Machine learning algorithms can be applied at the back of this techniquesin order to train and test the model which can be used to identify or classify the malware [32].

Although this technique performs with high accuracy of detection of early-stage malware to a reasonable level, it still lacks the capacity to detect complicated malwares. [32] presented a survey on the application of heuristic detection methods and machine learning algorithms, the study is aimed at providing detailed research on the features of a program like API calls, N-gram, CFG, opcode etc. this is done in order to overcome the disadvantages that are associated with signature and behavioral-based malware detection techniques.

IOT and Mobile based detection Technique

Internet of Things (IoT) devices refers to smart devices that are connected together with the help of the Internet, such devices can be home appliances, network cameras, and sensors. The IoT devices and mobile devices are more often commonly used than PCs. Since IoT and mobile devices are becoming more regular and commonly used among users on a daily basis, they are equally becoming more preferred to be attacked by hackers. Due to that, the focus of malware detection schemes is shifting from computers to IoT and mobile devices. [35] Gives the analysis of all currently known malwares families on the IoT platform and publishing them as an open-source material.

[36] Proposed a system that uses real-world datasets for classifying mobile applications and applies two feature selection methods like Chi–Square and ANOVA with 10 supervised ML algorithms for this classification. The result achieved from this system has a detection accuracy of 98.1%with a classification time of 1.22s on an average application. [31] Proposes an application behaviour- detection method based on multi feature and process algebra for detecting privilege escalation attacks in Android applications.

Machine Learning Detection Techniques

Machine Learning (ML) can provide malware prevention operations on a wireless network to detect and classify current, new and subtle attacks without the need for human-based training or intervention. It can be defined as a set of methods that detects patterns automatically and predict the trends for future data [37]. In the existence of various and enormous volume of machine learning techniques, the primary operation of them all is relied on the optimal features that it selects and this feature provides the metrics that will be used for the detection and classification of patterns and trends that can be categorized as malwares [38]. For example, one feature of a network is the packet size: machine learning techniques may monitor the packet size over time and generate distributions from which conclusions may be drawn regarding an intrusion [39].

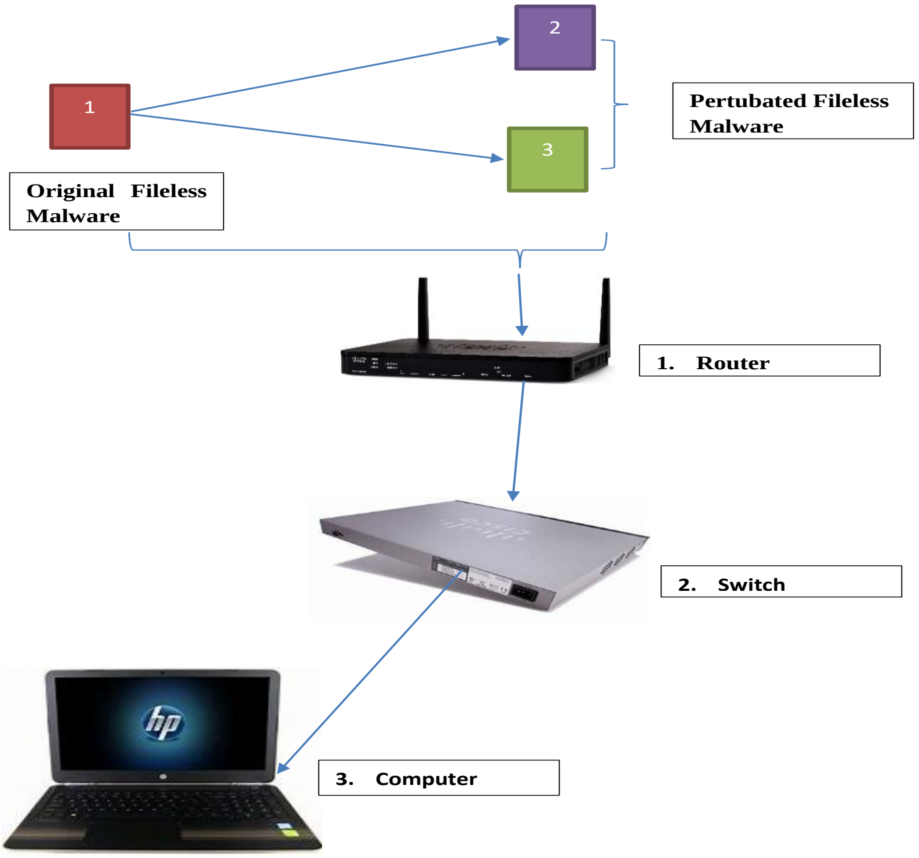
Adversarial Machine Learning Attacks and Detection Technique

Machine learning provides a means of solving complex problems and tasks effectively from spectrum data provided into the system on various fields and it can as well be very effective on the area of wireless communications [22] The recent advances in computational resources, algorithmic designs and problem solving have supported that deep learning has achieved a high level of success in performing deep tasks of various wireless communication types such as spectrum signaling and signal recognition effectively [28].

However, Limitations has been found on the field of machine learning in general and deep learning in particular has recently been found vulnerable to manipulations in training and test times giving rise to a field of study called Adversarial Machine Learning (AML). Although AML has been extensively studied in other data domains such as computer vision and natural language processing, research for AML in the wireless communications domain is in its early stage [40][41][42].

Attackers have also found a means to develop malwares that is capable of learning and adapting to solutions and creating new ways to launch attacks on various systems and this technique is identified as

Adversarial Attacks. According to [30] defined an adversarial attack the one that aims at the reduction of accuracy for malware detection models by the addition of perturbations in the malware samples to impose misclassification, this finally results to an increase in the fooling rate of the system.



Fileless Malware Flow

The square box with the number "1" represents the original fileless malware that has not been optimized. The square box with the number "2" and "3" represents two different types of optimization done on the original fileless malware called malware perturbation. When a fileless malware enters into a network, it land on the router or layer 3 switch. This is part of layer 3 (OSI model). The outbound access-list which is a firewall protecting the network from unauthorized IP addresses filters out unwanted IP addresses then the next line of firewall is the trained model. The optimized form of this fileless malware which is a new techniques used by malware authors usually bypasses this trained model meant to capture fileless malware. It moves to the switch which in turn directs it to the appropriate system where it will invoke the powershell or sometimes the WMI (Windows Management Instrumentation). After execution, it manipulates the powershell or the WMI to change privilege from the user privilege to either the super user privilege or the administrator's privilege. This gives the malware power to either whitelisting itself, inserting itself into a running memory or into the windows registry.

Adversarial Perturbation

In adversarial perturbation, one way the query input is changed from x to x' is through the method, where the perturbation is computed such that the prediction will not be the same as the original label [43][44]. Adversarial perturbation can be categorized into one-step and multi-step perturbation. As the names imply, the one-step perturbation only involves a single stage add noise once and that is it [45]. On the other hand, the multi-step perturbation is an iterative attack that makes small modifications to the input each time. Therefore, the one-step attack is fast but excessive noise may be added, hence making it easier for humans to detect the changes. Furthermore, it places more weight on the objective of maximizing loss and less on minimizing the amount of perturbation. Conversely, the multi-step attack is more strategic as it introduces small amounts of perturbation at each time. However, this also means such an attack is computationally more expensive [42][46].

V. DISCUSSION AND CONCLUSION

This study presented a review on the application of machine learning techniques for the elimination or control of file-less malware attack on a computer system of software platforms. The review started by presenting an overview of file-less malwares, types of the file-less malwares that can be encountered and various techniques adopted in tackling these challenges. The techniques presented in this work are signature—based technique, behavior-based technique, heuristic methods, IoT-based methods and machine learning methods. Further in the work, adversarial machine learning was introduced and how attackers implement this technique for the development of an intelligent malware that is capable of maneuveringother techniques. In this work, the application of machine learning (deep neural network) is presented as the most effective means that can be applied for an effective detection of this type of malware. Therefore, it is recommended that future research works should aim at adopting deep learning for the mitigation of adversarial malware attacks.

REFERENCES

[1]. Fortinet.Com (2023), Top 20 Most Common Types Of Cybersecurity Attacks. Online At Https://Www.Fortinet.Com/Resources/Cyberglossary/Types-Of-Cyber-Attacks Accessed May, 2023.

[2]. Patten D., (2017) The Evolution To File-Less Malware (2017). Http://Www.Infosecwriters.Com/Papers/Dpatten File-Less.Pdf.

[3]. Kumar S, Dohare U, Kumar K, Prasad Dora D, Naseerqureshi K, Kharel R (2019) Cybersecurity Measures For Geocasting In Vehicular Cyber Physical System Environments. IEEE Internet Things J 6(4):5916–5926. Https://Doi.Org/10.1109/ JIOT.2018.2872474

[4]. Living Off The Land Binaries And Scripts - (Lolbins And Lolscripts) (2019). Https://Github.Com/LOLBAS-Project/LOLBAS

[5]. Sudhakar R. And Kumar S. (2020) "An Emerging Threat File-Less Malware: A Survey And Research Challenges" Cybersecurity: Https://Doi.Org/10.1186/S42400-019-0043-X

[6]. Jeffrey C., Mahmoud A., And Maanak G., (2021) "Analyzing Machine Learning Approaches For Online Malware Detection In Cloud" Arxiv:2105.09268v1 [Cs.CR] 19 May 2021

[7]. Graeber M (2015) "Abusing Windows Management Instrumentation (WMI) To Build A Persistent, Asynchronous, And File-Less Backdoor", Black Hat, Las Vegas

[8]. Pontiroli S., & Martinez F., (2015) "The TAO Of .Net And Powershell Malware Analysis", In: Virus Bulletin Conference.

[9]. Afianian A, Niksefat S, Sadeghiyan B, Baptiste D (2018) "Malware Dynamic Analysis Evasion Techniques: A Survey", Arxiv Preprint Arxiv 1811:01190

[10]. Borkar Promod (2019), The New Breed Of "File-Less Malware" And How It Can Be Stopped With Behavioural Analytics And Machine Learning, Http://Www.Exabeam.Com/Ueba/File-Less-Malware-Behavioral-Analytics-Machine-Learning.

[11]. Le V., Welch I., Gao X., &Komisarczuk P., (2013) "Anatomy Of Drive-By Download Attack", Proceedings Of The Eleventh Australasian Information Security Conference (AISC 2013), Adelaide, Australia.

[12]. Johns, M. (2008), 'On Javascript Malware And Related Threats', Journal In Computer Virology 4(3), 161– 178.

[13]. Logix (2021) "Memory-Resident Malware: What You Should Know", Https://Logixconsulting.Com/2021/04/22/Memory-Resident-Malware-What-You-Should-Know/ Accessed December 2022.

[14]. Zou C., Gong W., Towsley D., (2002) "Code Red Worm Propagation Modeling And Analysis", In: Proceedings Of The 9th ACM Conference On Computer And Communications Security, Vol 147, P 138 ACM.

[15]. Rhodes KA (2001) Code Red, Code Red II, And Sircam Attacks Highlight Need For Proactive Measures. GAO Testimony Before The Subcommittee On Government Efficiency.

[16]. O'Murchu L, Gutierrez F., (2015) The Evolution Of The File-Less Click-Fraud Malware Poweliks. Symantec Corp.

[17]. Shulmin A., And Prokhorenko M., (2016) "Lurk Banker Trojan: Exclusively For Russia", Https://Securelist.Com/Lurk-Banker-Trojan-Exclusively-For-Russia/75040/

[18]. Rasa A., (2022) "Manually Recreatingthe Microsoft Office Follina Payload To Exploit Remote Systems (CVE-2022-30190)" Linkedin: Https://Www.Linkedin.Com/Pulse/Manually-Recreating-Microsoft-Office-Follina-Payload-Exploit-Rasa/ Accessed December 2022

[19]. Stella (2022) "How To Check The Windows Registry For Malware And Remove It", Minitool; Https://Www.Minitool.Com/News/Check-Registry-For-Malware-And-Remove-It.Html Accessed December 2022.

[20]. Wueest C., Anand H., (2017) "Living Off The Land And File-Less Attack Techniques", Https://Www.Symantec.Com/Content/Dam/Symantec/Docs/Security-Center/White-Papers/Istr-Living-Off-The-Land-And-File-Less-Attack-Techniques-En.Pdf.

[21]. Zeltser L (2017) "The History Of File-Less Malware-Looking Beyond The Buzzword"

[22]. Kang A., Jeong Y., Kim S., & Woo J., (2019) "Malicious PDF Detection Model Against Adversarial Attack Built From Benign PDF Containing Javascript", MDPI Appl. Sci. 2019, 9, 4764; Doi:10.3390/App9224764 Www.Mdpi.Com/Journal/Applsci

[23]. Ronghua T., (2011) "An Integrated Malware Detection And Classification System" In Workshop Proceedings Of Applications And Techniques In Information Security(ATIS).

[24]. Maiorca D., Biggio B., &Gaicinto G., (2020) "Towards Adversarial Malware Detection: Lessons Learned From PDF-Based Attacks", ACM Computing Surveys, Vol. 1, No. 1, Article 1. Publication Date: January 2019. Https://Doi.Org/10.1145/3332184

[25]. Xinbo L., Jiliang Z., Yaping L., He L. (2019) "(ATMPA: Attacking Machine Learning-Based Malware Visualization Detection Methods Via Adversarial Examples" 1808.01546v3 [Cs.CR] 30.

[26]. Moisejevs I., (2019) "Adversarial Attacks And Defenses In Malware Classification: A Survey", International Journal Of Artificial Intelligence And Expert Systems (IJAE), Volume (8) : Issue (3) : 2019 Pp 31-43.

[27]. Di X., Jingmei L., Tu L., Weifei W., Jiaxiang W., (2019) "Malware Classification Using Probability Scoring And Machine Learning", IEEE ACCESS; VOLUME 4, 2016; DOI10.1109/ACCESS.2019.2927552.

[28]. Aryal K., Gupta M., & Abdelsalam M., (2021) "A Survey On Adversarial Attacks For Malware Analysis", Arxiv:2111.08223v1 [Cs.CR] 16 Nov 2021.

[29]. Angelo C., Dentamaro V., Galantucci S., Iannacone A., Impedovo D., Pirlo G., (2021) "Comparing Deep Learning And Shallow Learning Techniques For API Calls Malware Prediction: A Study", Appl. Sci., 12, 1645. Https://Doi.Org/10.3390/App12031645.

[30]. Rathore H., Samavedhi A., Sahay S., & Sewak M., (2021) "Robust Malware Detection Models: Learning From Adversarial Attacks And Defenses", Forensic Science International: Digital Investigation Journal Homepage: Www.Elsevier.Com/Locate/Fsidihttps://Doi.Org/10.1016/J.Fsidi.2021.301183.

[31]. Limin Shen, Hui Li, Hongyi Wang, Yihuan Wang, "Multifeature-Based Behavior Of Privilege Escalation Attack Detection Method For Android Applications", Mobile Information Systems, Vol. 2020, Article ID 3407437, 16 Pages, 2020. Https://Doi.Org/10.1155/2020/3407437

[32]. Khushali V., (2022) "A Review On File-Less Malware Analysis Techniques", International Journal Of Engineering Research & Technology (IJERT) Http://Www.Ijert.Org ISSN: 2278-0181 IJERTV9IS050068 Www.Ijert.Org Vol. 9 Issue 05, May-2020 Pp 46-49

[33]. Ren Z., Wu H., Ning Q., Hussain I., & Chen B., (2020). "End-To-End Malware Detection For Android Iot Devices Using Deep Learning". Ad Hoc Networks. 101. 102098. 10.1016/J.Adhoc.2020.102098.

[34]. Bazrafshan Z., Hashemi H., Fard H., And Hamzeh A., (2013) "A Survey On Heuristic Malware Detection Techniques," The 5th Conference On Information And Knowledge Technology, Shiraz, 2013, Pp. 113-120, Doi: 10.1109/IKT.2013.6620049.

[35]. Alazab M., (2020) "Automated Malware Detection In Mobile App Stores Based On Robust Feature Generation." Electronics 9.3 (2020): 435.

[36]. Alazab M., Et Al. (2020) "Intelligent Mobile Malware Detection Using Permission Requests And Api Calls", Future Generation Computer Systems 107 (2020): 509-521.

[37]. Hodo X., Bellekens A., Hamilton P., Dubouilh E., Iorkyase C., Tachtatzis And Atkinson R., (2016) "Threat Analysis Of Iot Networks Using Artificial Neural Network Intrusion Detection System," 3rd International Symposium On Networks, Computers And Communications (ISNCC), 2016, Pp. 1–6

[38]. Mohammed A. A., Amr M., Abdulla A., Xiaojiang D. And Mohsen G. (2019). A Survey Of Machine And Deep Learning Methods For Internet Of Things (Iot) Security. NPRP Grant #8-408-2-172 From The Qatar National Research Fund (A Member Of Qatar Foundation.

[39]. He C., Tang Y., Yang Y., Qiao And Liu C., (2012) "3D-IDS: Iaas User-Oriented Intrusion Detection System," Information Science And Engineering (ISISE), 2012 International Symposium On, Pp. 12-15.

[40]. Liu Q., Guo J., Wen C., And Jin S., (2020) "Adversarial Attack On Dlbased Massive MIMO CSI Feedback," Journal Of Communications And Networks, Vol. 22, No. 3, Pp. 230–235, 2020.

[41]. Lin Y. Zhao H., Y. Tu, S. Mao, And Z. Dou, (2020) "Threats Of Adversarial Attacks In DNN-Based Modulation Recognition," In IEEE Conference On Computer Communications (INFOCOM).

[42]. Kim B., Y. E. Sagduyu, T. Erpek, K. Davaslioglu, And S. Ulukus, (2020) "Adversarial Attacks With Multiple Antennas Against Deep Learning-Based Modulation Classifiers," Arxiv Preprint Arxiv:2007.16204.

[43]. Sadeghi M., And Larsson E., (2019) "Physical Adversarial Attacks Against End-To-End Autoencoder Communication Systems," IEEE Communications Letters, Vol. 23, No. 5, Pp. 847–850.

[44]. Papernot N., Mcdaniel P., Wu X., Jha S., Swami A., (2016). "Distillation As A Defense To Adversarial Perturbations Against Deep Neural Networks", In: IEEE Symposium On Security And Privacy (S & P). IEEE, Pp. 582-597.

[45]. Kurakin A., Goodfellow I., Bengio S., (2017). "Adversarial Examples In The Physical World", In: International Conference On Learning Representations (ICLR).

[46]. Kokali-Filipovic R., Miller, And Vanhoy G., (2019) "Adversarial Examples In RF Deep Learning: Detection And Physical Robustness," In IEEE Global Conference On Signal And Information Processing (Globalsip).