

INTRODUCTION		MALWARE DETECTION TECHNIQUES																																					
<ul style="list-style-type: none">With new malwares coming every day, traditional detection techniques do not perform well and there is need for effective zero-day malware detection model		<ol style="list-style-type: none">Signature Based Technique : In this technique, the given malware is searched and matched with existing malwares in a malware definition database table. This technique faces challenges when malware uses code obfuscation.Static Analysis : Static analysis is a method that captures the information from the binary program without executing.Dynamic Analysis : Dynamic analysis is the process of monitoring malware behavior at run time in an isolated environment. Dynamic analysis can be an efficient long term solution for malware detection system. The Dynamic analysis cannot be deployed in end-point real time malware detection due to the reason that it takes much time to analyze its behavior, during which malicious payload can get delivered.Machine Learning : Machine learning algorithms (MLAs) rely on the feature engineering, feature selection and feature representation methods. The set of features with a corresponding class is used to train a model in order to create a separating plane between the benign and malwares. This separating plane helps to detect a malware and categorize it into its corresponding malware family.Deep Learning : During the training process, it tries to capture higher level representation of features in deep hidden layers with the ability to learn from mistakes. MLAs experience diminishing outputs as they see more and more data whereas deep learning captures new patterns and establishes associations with the already captured pattern to enhance the performance of tasks.																																					
OBJECTIVES																																							
<ul style="list-style-type: none">We propose a novel image processing technique with optimal parameters for MLAs and deep learning architectures to arrive at an effective zero-day malware detection model.We perform a comparative study of our model with other detection models.																																							
METHODOLOGY		PROPOSED ARCHITECTURE																																					
<ol style="list-style-type: none">A new proposal of a scalable and hybrid framework which facilitates to collect malware samples from different sources in a distributed way and to apply pre-processing in a distributed manner. The framework has the capability to process large number of malware samples both in real-time and on demand basis.A proposal of a novel image processing technique for malware classification.It follows two stage approach, in the first stage the executables file is classified into malware or legitimate using Static and Dynamic analysis and in second stage the malware executables file is categorized into corresponding malware family.An independent performance evaluation of classical MLAs and deep learning architectures, benchmarking various malware analysis models.		<p>The diagram illustrates the proposed malware detection architecture. It starts with four 'EXE' file icons representing raw malware samples. These are collected by a 'Distributed .EXE Collector' and stored in a 'NoSQL' database as 'Raw malware samples'. The samples are then processed by a 'Distributed .EXE Parser' to create 'Preprocessed malware samples'. These are fed into two parallel analysis modules: 'Windows-Dynamic-Brain-Droid (WDBD)' and 'Windows-Static-Brain-Droid (WSBD)'. Both modules output to a 'Malware' decision diamond. If the result is 'Yes', it triggers 'Continuous monitoring' and 'DeepImageMalDetect'. The 'DeepImageMalDetect' module also feeds into a 'Front End Broker', which leads to 'Visualization'. A 'NoSQL' database is also connected to the 'Malware' decision point.</p>																																					
		TYPES OF MALWARE																																					
		<p>The infographic titled 'Types of Malware' lists eight types with icons and descriptions: BUGS: A type of error, flaw or failure that produces an undesirable or unexpected result. Bugs typically exist in a website's source code and can cause a wide range of damage. WORMS: A worm relies on security failures to replicate and spread itself to other computers. They are often hidden in attachments and will consume bandwidth and overload a web server. VIRUS: A piece of code that is loaded onto your website or computer without your knowledge. It can easily multiply and be transmitted as an attachment or file. BOTS: A software program created to perform specific tasks. Bots can send spam or be used in a DDoS attack to bring down an entire website. TROJAN HORSES: Much like the myth, a Trojan disguises itself as a normal file and tricks users into downloading it, consequently installing malware. RANSOMWARE: Ransomware denies access to your files and demands payment through Bitcoin in order for access to be granted again. ADWARE: A type of malware that automatically displays unwanted advertisements. Clicking on one of these ads could redirect you to a malicious site. SPYWARE: A type of malware that functions by spying on a user's activity. This type of spying includes monitoring a user's activity, keystrokes and more.</p>																																					
		<p>The bar chart titled 'Malware growth' shows the 'Amount of Malware (in millions)' on the y-axis (0 to 400M) and 'Year' on the x-axis (2005 to 2015). It compares 'Total new malware' (blue bars) and 'Total malware' (grey bars). The data shows a significant upward trend, with total malware reaching nearly 400 million by 2015.</p> <table><tr><th>Year</th><th>Total new malware (M)</th><th>Total malware (M)</th></tr><tr><td>2005</td><td>~10</td><td>~10</td></tr><tr><td>2006</td><td>~15</td><td>~25</td></tr><tr><td>2007</td><td>~20</td><td>~35</td></tr><tr><td>2008</td><td>~25</td><td>~50</td></tr><tr><td>2009</td><td>~30</td><td>~70</td></tr><tr><td>2010</td><td>~40</td><td>~100</td></tr><tr><td>2011</td><td>~50</td><td>~140</td></tr><tr><td>2012</td><td>~60</td><td>~190</td></tr><tr><td>2013</td><td>~80</td><td>~270</td></tr><tr><td>2014</td><td>~100</td><td>~350</td></tr><tr><td>2015</td><td>~120</td><td>~400</td></tr></table>		Year	Total new malware (M)	Total malware (M)	2005	~10	~10	2006	~15	~25	2007	~20	~35	2008	~25	~50	2009	~30	~70	2010	~40	~100	2011	~50	~140	2012	~60	~190	2013	~80	~270	2014	~100	~350	2015	~120	~400
Year	Total new malware (M)	Total malware (M)																																					
2005	~10	~10																																					
2006	~15	~25																																					
2007	~20	~35																																					
2008	~25	~50																																					
2009	~30	~70																																					
2010	~40	~100																																					
2011	~50	~140																																					
2012	~60	~190																																					
2013	~80	~270																																					
2014	~100	~350																																					
2015	~120	~400																																					
CONCLUSIONS		REFERENCES/PUBLICATIONS																																					
<ul style="list-style-type: none">We would like to explore this topic further and learn more about how neural networks can be used for detection in malware.We have read a few papers about malware detection and would like to explore more papers about the same.We would also like to work on finding ways in which malware can be detected efficiently using the existing methods.		<ul style="list-style-type: none">Robust Intelligent Malware Detection Using Deep Learning - R. VINAYAKUMAR, MAMOUN ALAZAB, (Senior Member, IEEE), K. P. SOMAN, PRABAHARAN POORNACHANDRAN, AND SITALAKSHMI VENKATRAMAN<ul style="list-style-type: none">https://ieeexplore.ieee.orghttps://dl.acm.orghttps://springer.com/inhttps://sciencedirect.comhttps://researchgate.com																																					