Home (http://ipindia.nic.in/index.htm) About Us (http://ipindia.nic.in/about-us.htm) Who's Who (http://ipindia.nic.in/whos-who-page.htm)
Policy & Programs (http://ipindia.nic.in/policy-pages.htm) Achievements (http://ipindia.nic.in/achievements-page.htm)
RTI (http://ipindia.nic.in/right-to-information.htm) Feedback (https://ipindiaonline.gov.in/feedback) Sitemap (shttp://ipindia.nic.in/itemap.htm)
Contact Us (http://ipindia.nic.in/contact-us.htm) Help Line (http://ipindia.nic.in/helpline-page.htm)
Skip to Main Content Screen Reader Access (screen-reader-access.htm)

InPASS
Indian Patent Advanced Search System
(http://ipindia.nic.in/index.htm)
INTELLECTUAL PROPERTY INDIA
PATENTS | DESIGNS | TRADE MARKS
GEOGRAPHICAL INDICATIONS
(http://ipindia.nic.in/inc

Patent Search

Invention Title	STATIC MALWARE ANALYSIS USING DEEP LEARNING
Publication Number	12/2022
Publication Date	25/03/2022
Publication Type	INA
Application Number	202211013696
Application Filing Date	14/03/2022
Priority Number	
Priority Country	
Priority Date	
Field Of Invention	COMPUTER SCIENCE
Classification (IPC)	G06F0021560000, G06N0003040000, H04L0029060000, G06N0003080000, G06N0020000000

Inventor

Name	Address	Country	Nat
Amit Kumar Mishra	Assistant Professor, Department of CSE, Graphic Era Hill University, Uttarakhand, India, 248001 and (Ph.D. Scholar) Computer Science & Engineering Dept., Graphic Era deemed to be University, Dehradun, INDIA	India	Indi
Neha Tripathi	Assistant Professor, Department of CSE, Graphic Era Deemed to be University, Uttarakhand, India, 248001	India	Indi
Umang Garg	Assistant Professor, Department of CSE, Graphic Era Hill University, Uttarakhand, India, 248001	India	Indi
Vikram Singh Soni	Sr. Lab Assistant, Department of ECE, Graphic Era Deemed to be University, Uttarakhand, India, 248001	India	Indi
Piyush Bagla	Ph.D. Scholar, Computer Science & Engineering Dept., National Institute of Technology, Jalandhar, Punjab - 144011	India	Indi
Dr. Neeraj Kumar Pandey	Assistant Professor, School of Computing, DIT University, Dehradun, Uttarakhand, India, 248001	India	Indi

Applicant

Name	Address	Country	Nat
Amit Kumar Mishra	Assistant Professor, Department of CSE, Graphic Era Hill University, Uttarakhand, India, 248001 and (Ph.D. Scholar) Computer Science & Engineering Dept., Graphic Era deemed to be University, Dehradun, INDIA	India	Indi
Neha Tripathi	Assistant Professor, Department of CSE, Graphic Era Deemed to be University, Uttarakhand, India, 248001	India	Indi
Umang Garg	Assistant Professor, Department of CSE, Graphic Era Hill University, Uttarakhand, India, 248001	India	Indi
Vikram Singh Soni	Sr. Lab Assistant, Department of ECE, Graphic Era Deemed to be University, Uttarakhand, India, 248001	India	Indi
Piyush Bagla	Ph.D. Scholar, Computer Science & Engineering Dept., National Institute of Technology, Jalandhar, Punjab - 144011	India	Indi
Dr. Neeraj Kumar Pandey	Assistant Professor, School of Computing, DIT University, Dehradun, Uttarakhand, India, 248001	India	Indi

Abstract:

There are two main components of malware analysis. One is static malware analysis and the other is dynamic malware analysis. Static malware analysis involves examinin basic structure of the malware executable without executing it, while dynamic malware analysis relies on examining malware behaviour after executing it in a controlled environment. Static malware analysis is typically done by modern anti-malware software by using signature-based analysis or heuristic-based analysis. This patent propos use of deep neural networks to learn features from a malware's portable executable (PE) to minimize the occurrences of false positives when recognizing new malware. W the EMBER dataset for training our model and compare our results with other known malware datasets. We show that using a simple deep neural network for learning ve PE features is not only effective, but is also less resource intensive as compared to conventional heuristic detection methods. Our model achieves an Area Under Curve (A 99.8% with 98% true positives at 1% false positives on the Receiver Output Characteristics (ROC) curve.

Complete Specification

The concept of malware detection mainly deals with analyzing executable files to establish malicious intent. Since the advent of anti-malware software, we have seen a rise in sophisticated malware which are specifically designed to circumvent this software. This in turn has spearheaded research into more advanced detection techniques. Malware analysis or malware detection can be performed in two ways: statically, and dynamically.
Static Malware Detection: Static malware detection is the process of analyzing a binary file without executing it. This can involve disseminating the _le entirely and examining every component, using a disassembler to reverse engineer it, or converting it into assembly code to examine its flow. It can also extend to the original source code of the software if available. This is usually the first line of defense against malware used by all anti-malware software.
Dynamic Malware Detection: Dynamic malware detection uses behavior analysis while a malware is running to determine malicious intent. Usually, this is done in a sandbox environment to ensure that the executable does not cause any harm to

View Application Status

Terms & conditions (http://ipindia.gov.in/terms-conditions.htm) Privacy Policy (http://ipindia.gov.in/privacy-policy.htm)
Copyright (http://ipindia.gov.in/copyright.htm) Hyperlinking Policy (http://ipindia.gov.in/hyperlinking-policy.htm)
Accessibility (http://ipindia.gov.in/accessibility.htm) Archive (http://ipindia.gov.in/archive.htm) Contact Us (http://ipindia.gov.in/contact-us.htm)
Help (http://ipindia.gov.in/help.htm)

Page last updated on: 26/06/2019