JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Detection of Malicious Documents and Websites Using Application Programming Interface

[1]Hrishikesh Bhor, [2]Prof. Priya N.

[1]Student, School of Computer Science & Information Technology,
[2]Assistant Professor, School of Computer Science & Information Technology
Jain Deemed to be University, Bangalore, India
Email: [1]bhorhrishikesh@gmail.com, [2]n.priya@jainuniversity.ac.in

Abstract: For detecting and blocking malicious and harmful files, antivirus software is one among the foremost commonly used programs. Antiviruses supported hosts, however, aren't as effective long-term. Today's antivirus software has become increasingly complex, leading to vulnerabilities which may be exploited by malware. a number of these vulnerabilities aren't detected by standard antivirus software. Now a days thanks to increase in internet uses the attacker finds news ways to hack or to realize access of a computing system. thanks to these new methods the utilization of antivirus programs is increasing day by day. These antivirus programs protect computing system and therefore the files present thereon system. Antivirus also protects the files which are being download from internet by scanning it. to see any malicious content hidden therein file. But when it involves internet not only the files are malicious but it also can be the online site or the web server. Now a days the hacker has acknowledged multiple new ways to trick the victim. Now a days most of the days the attacker makes use of the fake websites, web servers. and a few malicious URL's to fool people. This feature makes use of an Application Programming Interface to detect the malicious code inside the web site and scans the websites. URLs, and Ip addresses which appears to be legitimate but aren't.

***Keywords* - API, Worms, Malicious code, Trojan, Antivirus, JavaScript, Website Malware**

I. INTRODUCTION

Detecting malicious software system and infected files is also a tricky job. thanks to latest technologies the ways that} of concealment malicious code are terribly easy. These files are often scanned through antivirus which makes it safe to use. However the antivirus program cannot scan for the websites which you visit or surf on. in line with recent studies 30,000 websites are hacked on a daily basis and these websites is wont to inject some malicious code into the victim's computer once he surfs them. The machine-controlled tools make it additional easier to realize access of the websites. because the utilization of net is growing day by day the utilization of net applications is in addition victimisation rapidly. the typical folks doesn't have abundant plan concerning the we tend to sites however they work, what's running within the backend or on the server side. This makes it additional easier to fool them by creating them visit some malicious websites. the foremost common attack won't to fool is phishing attack wherever it's terribly troublesome to analyse that s real or fake. To avoid this instance what we really scan for the malicious websites which we've a doubt so as that we are safe from the hacker's malicious intentions. an internet site that is gaining attention is exploited by the attacker. the bulk of the hackers have intentions to steal users' non-public data, some private info like payment details of the user and generally it conjointly makes victim to forcefully be part of a malware distributes network. the net browsers support integration of multiple languages from which JavaScript is that the most generally utilized in active and dynamic web content creation which also provides a good probability for the exploits to be written easily. additional exploitation techniques embrace PHP, adobe flash player, and visual basics scripts which are terribly ordinarily downloaded and exploited.

II. OBJECTIVE: -

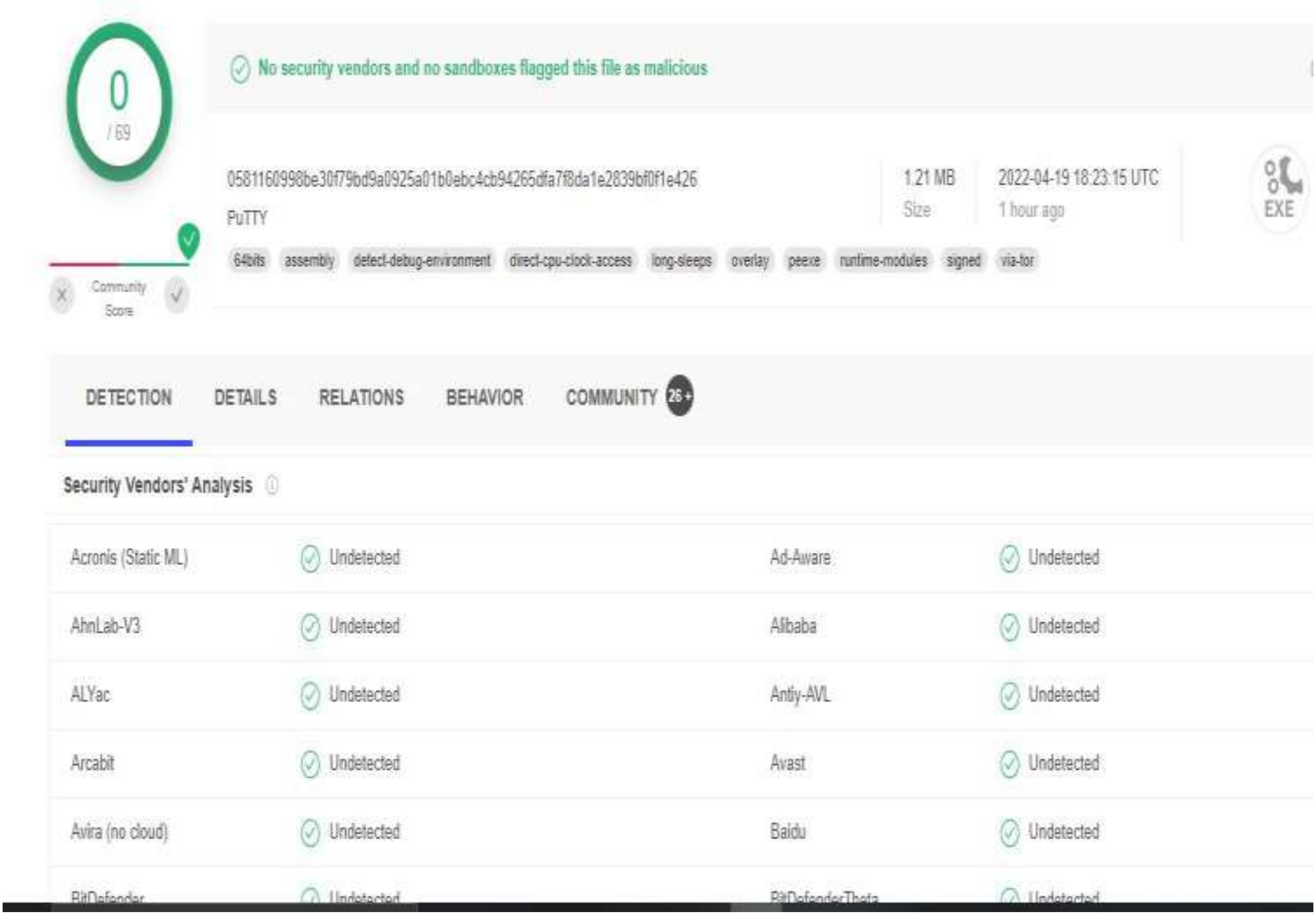
The objective of this design is to find out the malicious codes hidden inside a file or hidden on an website with using an application programming interface. The attackers find out new methods to gain unauthorized access or to gain some confidential data about the common users. Mostly used antivirus software can find out the whether the file is malicious or not but it cannot scan for the malicious content present on the website which we are visiting. To remain safe from such type of situation, if we can also be able to scan the websites which contains some malicious content or knew about reported as the malicious website using some tools.

III. PROPOSED SYSTEM: -

Application programming interface is a set of instructions or rules that allow access data and interact with external software components, operating systems and some micro services. In simple terms an application programming interface interact with system and provides input to the system and responds the request back to the user. Application Programming Interface acts as a gateway for enterprise's digital assets. These allows enterprises or organizations to quickly build a consumer experience. API's also opens new revenue channels for the organization or the developer who is making it or using in his project or software. Many of the developers tried to solve the problem of these malicious website's detection in multiple ways. Some tried with using the artificial intelligence, some tried with different algorithms etc. The malicious websites can sometimes ask you to download some software or a file to save or run it. This is the basic identification technique to find out which website is legitimate and which one is malicious or harmful. The attackers find out many ways to gain access to the users important and confidential data. These attackers insert some malicious code into to website so that they gain access to the users' confidential data. Users may get the notification to update their browser, or trick users by showing that their pc is infected with some type of virus and force them to download the software. These techniques can trick many users to get fool and fall for it. Even many legitimate websites get hacked or attacked by the hacker so that he can use it for his malicious intention. Many methods are used for the detection of the malicious websites, but mainly are the methods that are observed and then taken actions. These methods can also fail sometimes to detect the malicious content present on the website. By making use of an application programming interface, we can easily scan for the websites before visiting them. These minimize the risk of getting affected or losing some personal data. The application programming interface collects the data from multiple antivirus that are famous and mostly used. These results will help to identify and judge which websites are malicious and which are not. Not only websites we can also scan for the infected files and doubtful Ip addresses to scan and verify them.

IV. Results: -

-



0 / 69

Community Score

No security vendors and no sandboxes flagged this file as malicious

0581160998be30f79bd9a0925a01b0ebc4cb94265dfa7f8da1e2839bf0f1e426

PuTTY

1.21 MB
Size

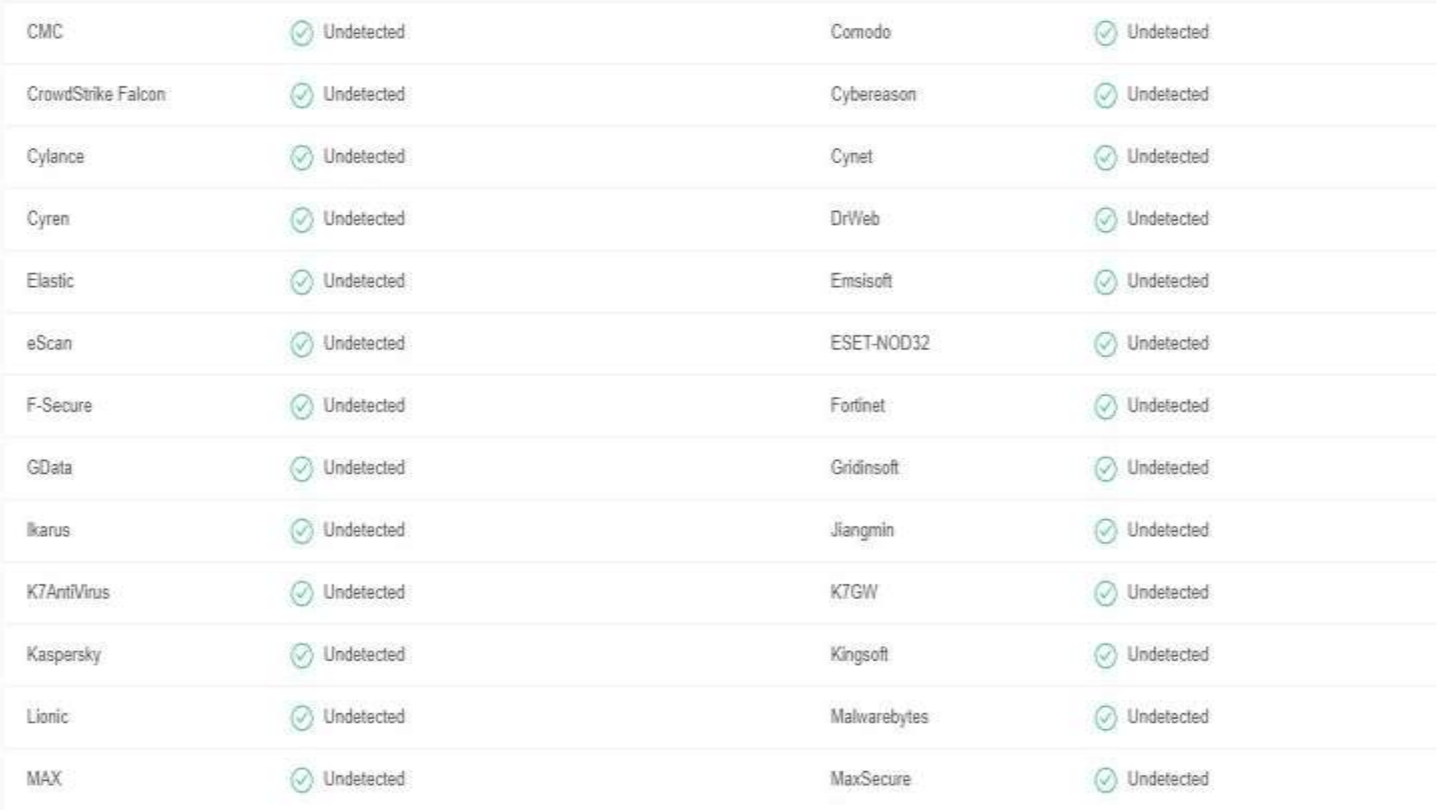
2022-04-19 18:23:15 UTC
1 hour ago

EXE

64bits · assembly · detect-debug-environment · direct-cpu-clock-access · long-sleeps · overlay · peexe · runtime-modules · signed · via-tor

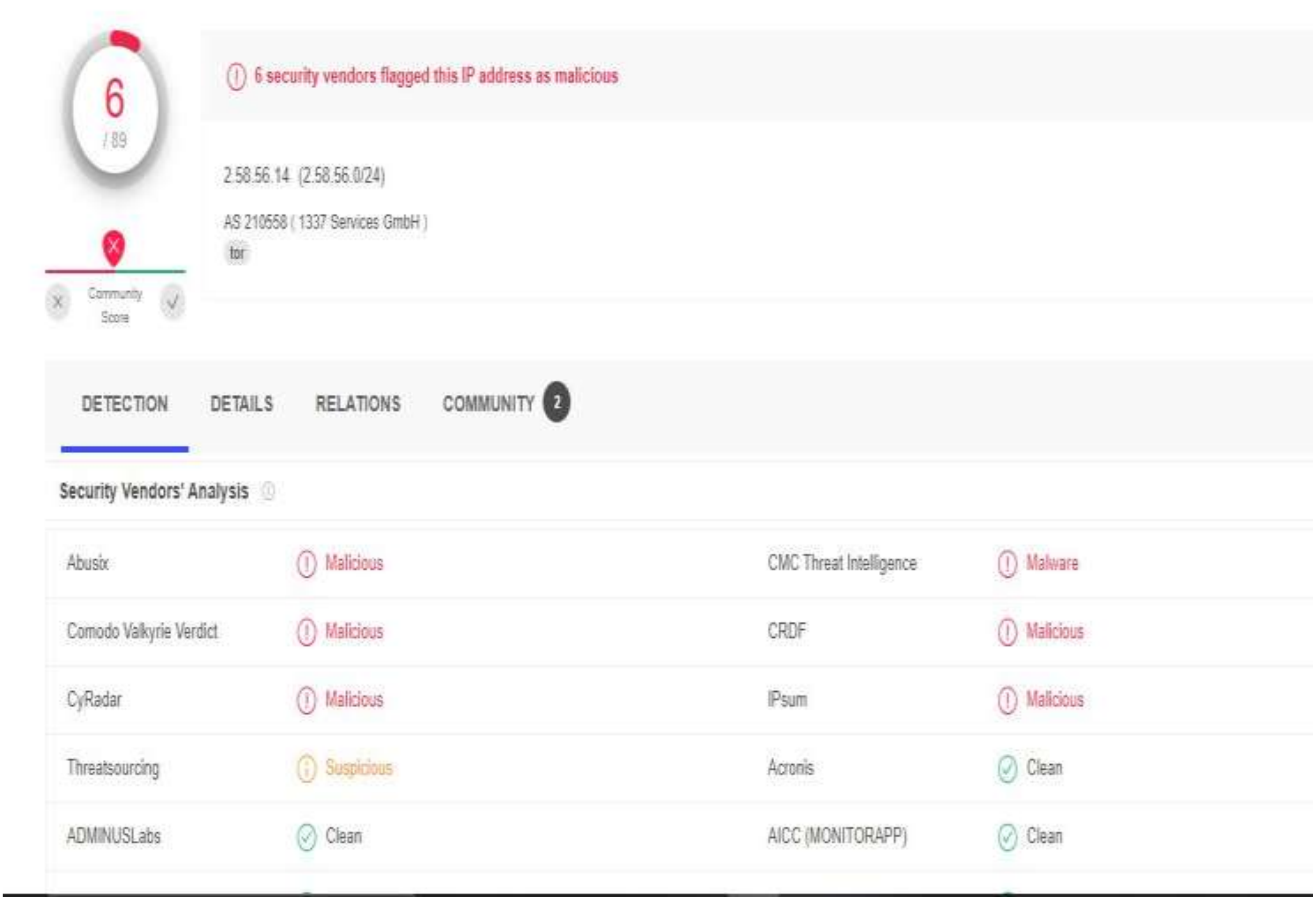
Security Vendors' Analysis

Acronis (Static ML)	Undetected	Ad-Aware	Undetected
AhnLab-V3	Undetected	Alibaba	Undetected
ALYac	Undetected	Antiy-AVL	Undetected
Arcabit	Undetected	Avast	Undetected
Avira (no cloud)	Undetected	Baidu	Undetected
BitDefender	Undetected	BitDefenderTheta	Undetected



CMC	✓ Undetected	Comodo	✓ Undetected
CrowdStrike Falcon	✓ Undetected	Cybereason	✓ Undetected
Cylance	✓ Undetected	Cynet	✓ Undetected
Cyren	✓ Undetected	DrWeb	✓ Undetected
Elastic	✓ Undetected	Emsisoft	✓ Undetected
eScan	✓ Undetected	ESET-NOD32	✓ Undetected
F-Secure	✓ Undetected	Fortinet	✓ Undetected
GData	✓ Undetected	Gridinsoft	✓ Undetected
Ikarus	✓ Undetected	Jiangmin	✓ Undetected
K7AntiVirus	✓ Undetected	K7GW	✓ Undetected
Kaspersky	✓ Undetected	Kingsoft	✓ Undetected
Lionic	✓ Undetected	Malwarebytes	✓ Undetected
MAX	✓ Undetected	MaxSecure	✓ Undetected

Fig 1. File scanning result(.exe)



6 security vendors flagged this IP address as malicious

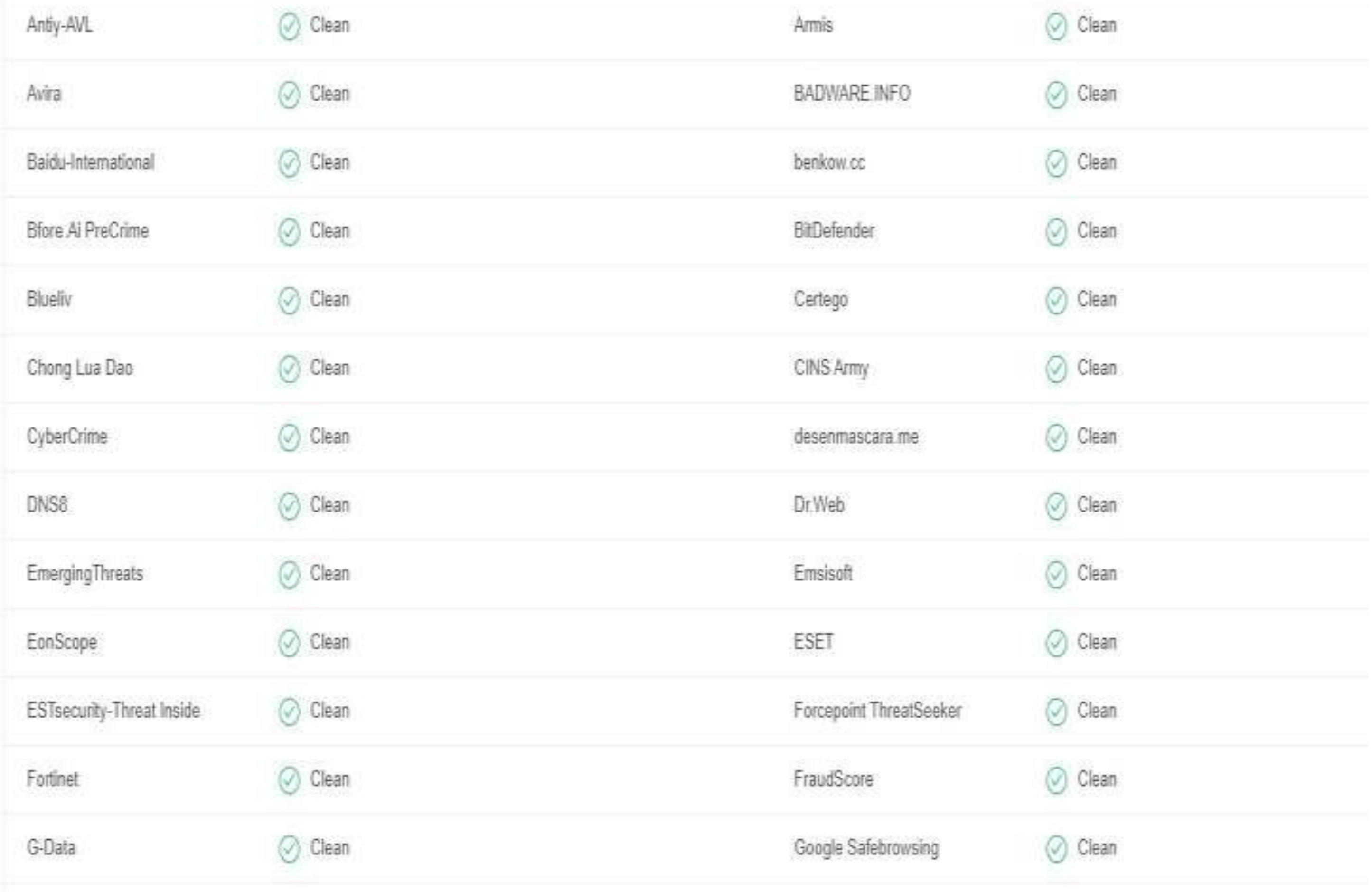
2.58.56.14 (2.58.56.0/24)

AS 210558 (1337 Services GmbH)

tor

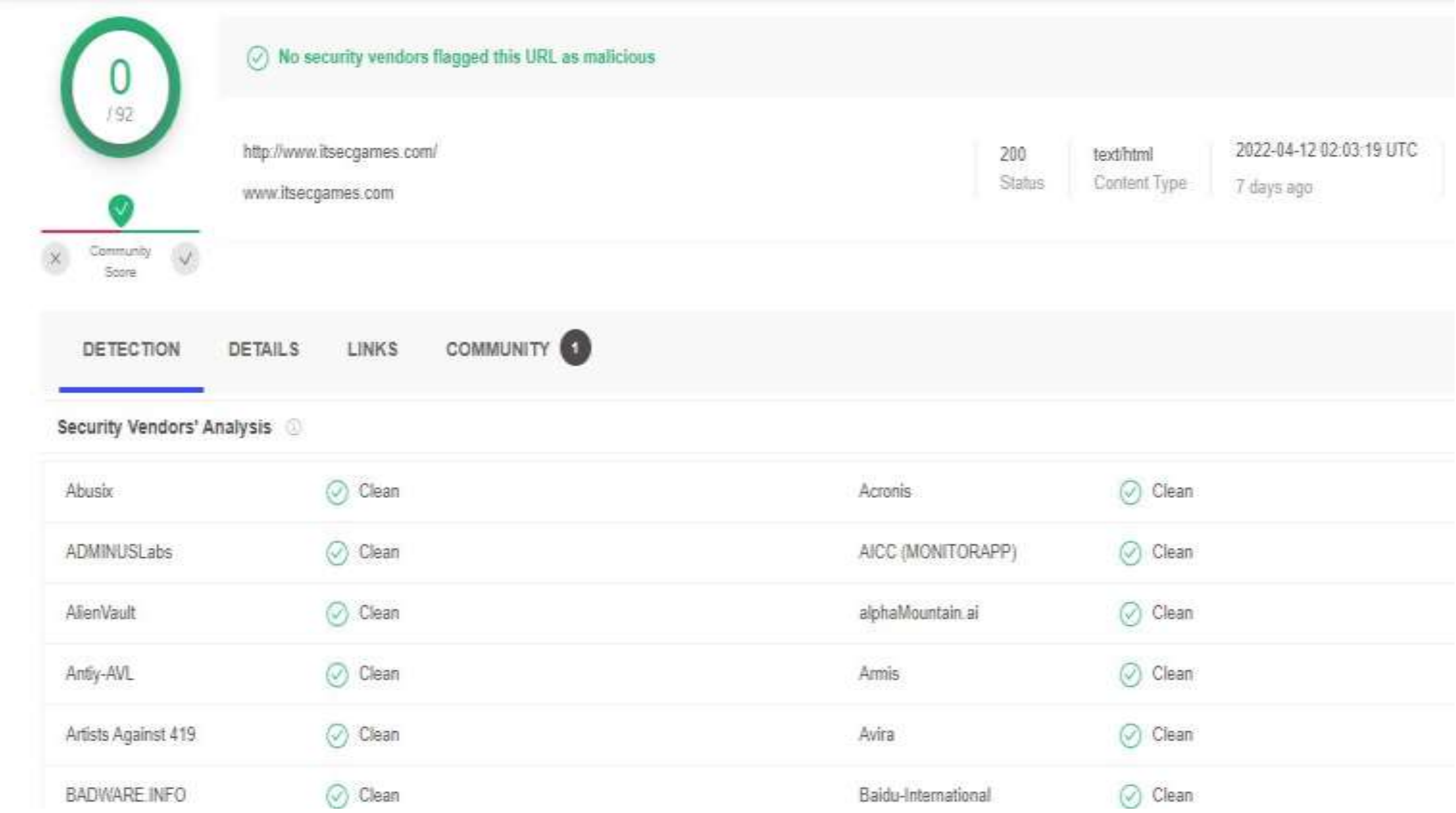
Security Vendors' Analysis

Abusix	Malicious	CMC Threat Intelligence	Malware
Comodo Valkyrie Verdict	Malicious	CRDF	Malicious
CyRadar	Malicious	IPsum	Malicious
Threatsourcing	Suspicious	Acronis	✓ Clean
ADMINUSLabs	✓ Clean	AICC (MONITORAPP)	✓ Clean



Antiy-AVL	✓ Clean	Armis	✓ Clean
Avira	✓ Clean	BADWARE.INFO	✓ Clean
Baidu-International	✓ Clean	benkow.cc	✓ Clean
Bfore.Ai PreCrime	✓ Clean	BitDefender	✓ Clean
Blueliv	✓ Clean	Certego	✓ Clean
Chong Lua Dao	✓ Clean	CINS Army	✓ Clean
CyberCrime	✓ Clean	desenmascara.me	✓ Clean
DNS8	✓ Clean	Dr.Web	✓ Clean
EmergingThreats	✓ Clean	Emsisoft	✓ Clean
EonScope	✓ Clean	ESET	✓ Clean
ESTsecurity-Threat Inside	✓ Clean	Forcepoint ThreatSeeker	✓ Clean
Fortinet	✓ Clean	FraudScore	✓ Clean
G-Data	✓ Clean	Google Safebrowsing	✓ Clean

Fig 2. Scanning result of an Ip address.



✓ No security vendors flagged this URL as malicious

http://www.itsecgames.com/
www.itsecgames.com

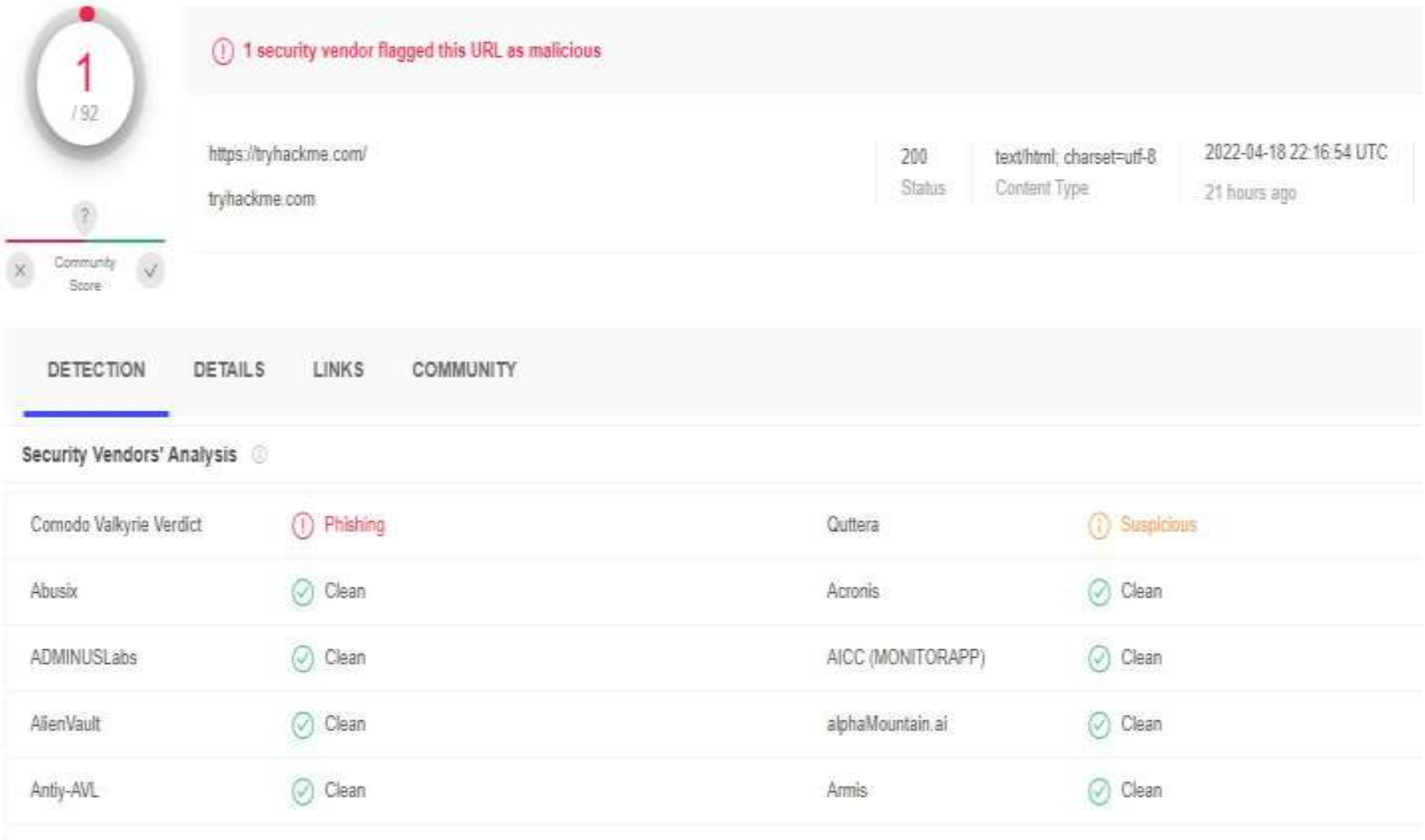
200 Status

text/html Content Type

2022-04-12 02:03:19 UTC
7 days ago

Security Vendors' Analysis

Abusix	✓ Clean	Acronis	✓ Clean
ADMINUSLabs	✓ Clean	AICC (MONITORAPP)	✓ Clean
AlienVault	✓ Clean	alphaMountain.ai	✓ Clean
Antiy-AVL	✓ Clean	Armis	✓ Clean
Artists Against 419	✓ Clean	Avira	✓ Clean
BADWARE.INFO	✓ Clean	Baidu-International	✓ Clean



1 security vendor flagged this URL as malicious

https://tryhackme.com/
tryhackme.com

200 Status	text/html; charset=utf-8 Content Type	2022-04-18 22:16:54 UTC 21 hours ago	

Security Vendors' Analysis

Comodo Valkyrie Verdict	Phishing	Quttera	Suspicious
Abusix	Clean	Acronis	Clean
ADMINUSLabs	Clean	AICC (MONITORAPP)	Clean
AlienVault	Clean	alphaMountain.ai	Clean
Antiy-AVL	Clean	Armis	Clean

Fig 3. Scanning results of websites

V. CONCLUSION

A simple model which may detect a malicious website, can also scan for the files to allow you to know is it infected or not and can also scan for the Ip addresses which are harmful for the users. it's clear that it's possible to detect for the malicious websites in a very simple way with the utilization of an application programming interface. Many of the key features are easy to use and available easily so that any user can use it without any difficulty. Many techniques have been introduced to find out whether the website is legitimate or not. But these methods cannot be 100% correct. As the hackers find out multiple new ways to fool or trick user to compromise its data. Using an application programming interface makes it easy to rectify whether it's legit or not.

VI. REFERENCES: -

[1] Soft-pedal, 2016. More than Half of the World's Malicious Websites Are Hosted in the US. [online] Available at: https://news.softpedia.com/news/more-than-half-of-the-world-s-malicious-websites-are-hosted-in-the-us-503210.shtml [Accessed 25 Feb. 2020].

[2] Website malware Available at: HTTPs://sucuri.net/guides/website-malware/

[3] Ikinci, A., 2008. Monkey-Spider: Detecting Malicious Websites with Low-Interaction Honeyclients. pp.407–421.

[4] Heiderich, M., Frosch, T. and Holz, T., 2011. IceShield: Detection and mitigation of malicious websites with a frozen DOM. In: Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). Springer, Berlin, Heidelberg.pp.281–300.

[5] Malicious website detection: A machine learning approach available at: https://link.springer.com/chapter/10.1007/978-3-642-41674-3_32

[6] Malicious website Detection: Effectiveness and Efficiency Issues available at: https://ieeexplore.ieee.org/document/6092782

[7] Detecting Malicious Websites Using Machine Learning available at: htt ps://scholarworks.rit.edu/cgi/viewcontent.cgi?article=11869&context=theses

[8] Analyzing and Exploiting Network Behaviours of Malware available at: https://link.springer.com/chapter/10.1007/978-3-642-16161-2_2

[9] Static detection of malicious JavaScript available at: https://dl.acm.org/doi/abs/10.1145/2076732.2076785

[10] Automated malicious advertisement detection using Virus Total, using URLVoid and trend micro. Available at: https://ieeexplore.ieee.org/abstract/document/7921994

[11] Chiba, D., Tobe, K., Mori, T. and Goto, S., 2012. Detecting malicious websites by learning IP address features. In: Proceedings - 2012 IEEE/IPSJ 12th International Symposium on Applications and the Internet, SAINT 2012. pp.29–39.

[12] Anon n.d. United States Patent: 8850570. [online] Available at: http://patft.uspto.gov/netacgi/nphParser?Sect1=PTO1&Sect2=HITOFF&d=PALL&p=1&u=%2Fnetahtml%2FPTO%2Fsrchnum.htm&r=1&f=G&l=50&s1=8850570.PN.&OS=PN/8850570&RS=PN/8850570