International Research Journal of Advanced Engineering and Science
ISSN (Online): 2455-9024

Using Shodan and Shodan API as a Vulnerability Tool for Security Testing

Micah Roble[1], Munther Abualkibash[2]
[1]School of Information Security and Applied Computing, Eastern Michigan University, Ypsilanti, Michigan, United States-48197
[2]School of Information Security and Applied Computing, Eastern Michigan University, Ypsilanti, Michigan, United States-48197

Abstract— *Technological advancement has led to the expansion of internet connected technologies. This includes expansions into industrial control systems, databases, artificial intelligence, internet of thing devices, smart homes, and autonomous vehicles. Databases in particular have gone through rapid expansion and development and are now used in every major organization in the world. Relational, object relational, and non-relational databases have all evolved over the course of the past two decades resulting in an abundance of variance in data management. Variance has allowed databases to be used in multiple different fields and occupations. Databases are being used to store accounting information, health information, statistics, and more. The extensive use of databases however has led to the mismanagement of databases and vulnerabilities related to databases are constantly arising. Vulnerable databases include MongoDB and Riak. These two databases are commonly used, especially in the case of MongoDB. Due to mismanagement, these databases are constantly targeted by attackers. Shodan is a search engine tool that is capable of discovering multiple vulnerable databases. For the improvement of security practices, the awareness of vulnerable databases needs to be emphasized so that common practices can be improved to reduce the short comings of unsecure databases. Multiple experiments were conducted to revel how potentially easy it is to discover vulnerable databases on Shodan and Shodan's capabilities to retrieve data. Through this research it is hoped that security practices for the management of databases will improve and reduce the possibilities of future possible database security breaches.*

Keywords— *Databases, Cyber security, Shodan, Database Security, Internet of Things.*

I. INTRODUCTION

The advancement in the internet and wireless technologies has also lead to the advancement of hackers and online threats and vulnerabilities. Every year cyber-attacks against business, nations, and NGO's result in the loss of Billions of dollars. 20 years ago, hackers were seen as mysterious intelligent figures who had advanced technical knowledge on computers and computer systems. These individuals would spend time researching systems and vulnerabilities, pioneering modern day black hat and white hat hacking. Times however have changed since the start of the cyber revolution. Hacking has become a much more lucrative field for both cyber security professionals and for those who would wish to steal or bring harm to an organization. The art of offensive security/hacking has grown into an active war into who can discover a vulnerability first and either patch it or exploit it. Many hackers today are amateurs and hobbyists who can use tools found online to assist the facilitation of hacking. Due to the expansion of technology, security professionals are constantly assessing the safety of organizations. Shodan, a search engine capable of discovering information on internet connected devices, is becoming a tool that security professionals can use to try to mitigate possible security vulnerabilities. This paper contains 5 sections including the Introduction. Section II will describe some of the searchable databases on Shodan (Riak and MongoDB) and the discovery of vulnerable banner information within Shodan. Section III describes weaknesses and potential exploits related to Riak and MongoDB, and in section IV I describe ways using Shodan and the Shodan API can be used by security professionals to help mitigate potential security threats to an organization

II. RELATED WORKS

Other papers the delve into similar topics include Abnormal Behavior-Based Detection of Shodan and Censys-Like Scanning-2017, Analyzing Internet-connected industrial equipment-2018, and a Research on the Vulnerabilities of PLC using Search Engine-2019

III. DATABASES

A. Databases on Shodan

There are numerous database that are contained within Shodan. This includes relational database management systems (RDBMS) like MySQL, object relational database management systems (ORDBMS) like PostgreSQL, and non-relational models for storing data (NoSQL) like MongoDB. Newer NoSQL databases have been known to have possible security vulnerabilities and MongoDB is no exception.

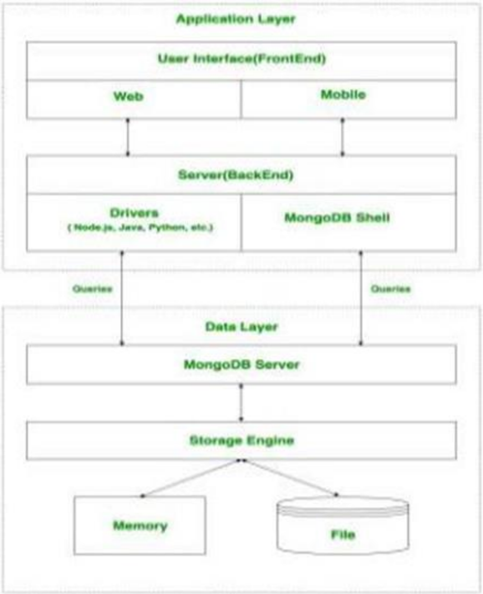


Fig. 1. MongoDB Basic Use Description

MongoDB has an especially vulnerable history when in comparison to other databases. Historically, MongoDB listened on public network interfaces which resulted in numerous MongoDB users unknowingly making their data viewable to anyone on the internet. Vulnerabilities that are related to databases are incredibly crucial to organizational security and can lead to disastrous consequences if not properly secured. Every kind of database, relational or non-relational is used to assist in the storing and retrieval of information. As computer systems improved and organizations grew, the use of databases has become common for every major business and organization on the planet. Due to the growth of businesses, databases have also increased in the amount of assets that they contain. A Riak server for instance can be astronomically useful with its fault tolerance, operational simplicity, low cost and its incredibly easy scalability. However, the appeal of Riak, MongoDB and other open-source database, has led to the threat of hackers attacking these databases to gain information on assets as to either cripple a business, or ruin the image of an organization. By using Shodan, one can immediately get information on websites that are using specified databases. This can be a useful tool for security professionals to check that their databases are secure but can also be used by attackers to scan for potential targets.

B. Shodan

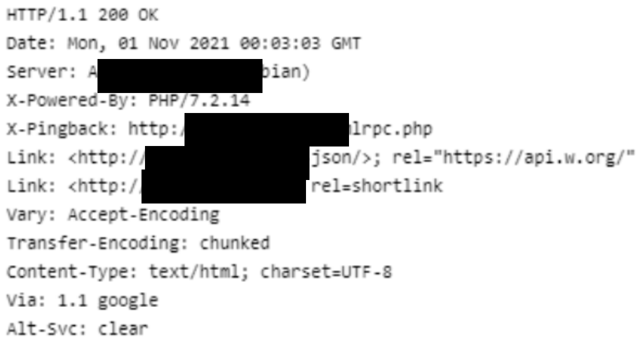
Shodan is the world's first search engine for Internet-connected devices. Discover how Internet intelligence can help you make better decisions.

Fig. 2. Shodan Dashboard

Shodan is a search engine that searches for devices connected to the internet. This however is not just limited to web applications and routers. Shodan has the ability to see servers, internet of things devices, baby monitors, cameras, industrial controls systems and more. Sensitive information can be retrieved by Shodan which makes it a very valuable tool for security professionals. Shodan was not made by hackers or meant for hackers. It is mainly used by security professionals for examining what devices are secure and if devices that appear on Shodan need to be secured. Many fourteen 500 companies are beginning to see the use of Shodan, and it is reported that 89% of fortune 100s use Shodan in some compacity. Even though Shodan is meant to be used by professionals, that does not deter harmful actors from using the information found on Shodan for malicious means.

Shodan's development started in 2003 by John Matherly. Matherly created an algorithm for a web crawler to constantly be crawling the internet for random IPv4 addresses. Creating this algorithm led to a rapidly increasing and large database of internet connected devices. This ever-increasing database was then publicly released in 2009, being marketed as a tool for IT and security professionals to secure their systems.

One of the key components of Shodan's data collection is the use of banner grabbing. A banner is described as metadata about a service. Banners usually contain various forms of useful information and can differ depending on the type of service. One common use of examining banners on Shodan is that banners can tell whether a service has authentication disabled. A typical banner can be seen in [Fig 3]to the overwhelming number of benign records, however, the authors conclude that there are too few attack vectors to be useful to an intrusion detection system.

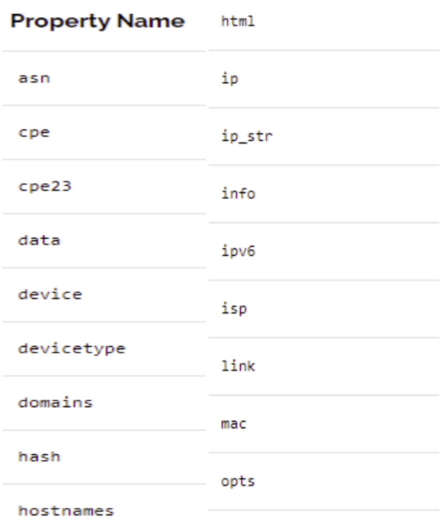


```
HTTP/1.1 200 OK
Date: Mon, 01 Nov 2021 00:03:03 GMT
Server: A[redacted]bian)
X-Powered-By: PHP/7.2.14
X-Pingback: http:/[redacted]lrpc.php
Link: <http:/[redacted]json/>; rel="https://api.w.org/"
Link: <http:/[redacted]rel=shortlink
Vary: Accept-Encoding
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8
Via: 1.1 google
Alt-Svc: clear
```

Fig 3. Banner

Shodan's capabilities are not just limited to grabbing basic banner information. Further data such as open ports, geographic locations, host names, operating systems, ISPs, web technologies, and more can be contained within a single Shodan result. Ports are selected through the algorithm by examining commonly used ports and services. Once a banner is intercepted by the Shodan crawler, it will continuously be crawled from Shodan to ensure the most up to date information is presented in the banner.

Banner grabbing can also be further used and filtered on Shodan to help provide a more focused searched. Some specified banner searches can include filtering for a specific ISP, device name, IP, and more. Examples of some banner property names can be seen in [Fig 4] Another feature of Shodan is the Shodan API and the paid for enterprise version of the Shodan API which can improve the use of banner grabbing, potentially grabbing thousands of results.



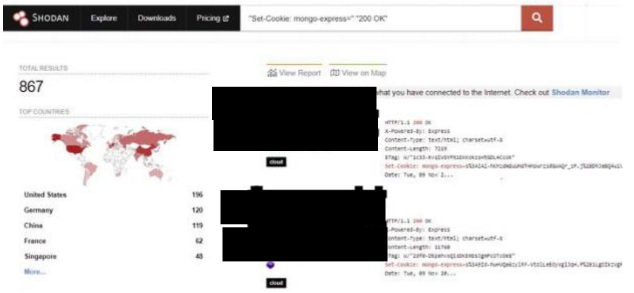
Property Name	html
asn	ip
cpe	ip_str
cpe23	info
data	ipv6
device	isp
devicetype	link
domains	mac
hash	opts
hostnames	

Fig. 4. Shodan Banner Filter

IV. MONGODB AND RIAK VULNEREABILITES

A. Discovering MongoDB vulnerabilities using Shodan

MongoDB most commonly uses the port 27017, 27018, and 27019 by using the filter "Set-Cookie: mongo-express=" "200 OK"" Shodan can filter for MongoDB servers that have open databases



SHODAN Explore Downloads Pricing "Set-Cookie: mongo-express=" "200 OK"

TOTAL RESULTS 867

TOP COUNTRIES

United States	196
Germany	120
China	119
France	62
Singapore	43
More...	

View Report View on Map

[redacted] what you have connected to the Internet. Check out Shodan Monitor

```
HTTP/1.1 200 OK
X-Powered-By: Express
Content-Type: text/html; charset=utf-8
Content-Length: 7219
ETag: [illegible]
Set-Cookie: mongo-express=[illegible]
Date: Tue, 09 Nov 2...
```

cloud

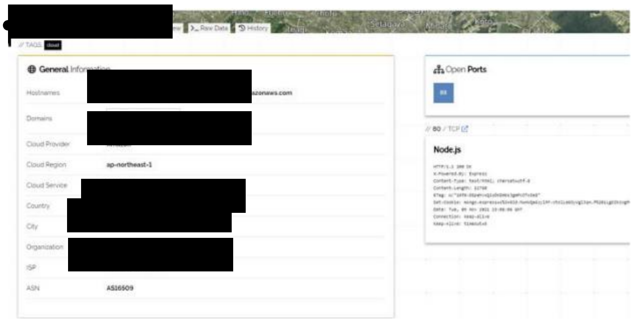
[redacted]

```
HTTP/1.1 200 OK
X-Powered-By: Express
Content-Type: text/html; charset=utf-8
Content-Length: 11760
ETag: [illegible]
Set-Cookie: mongo-express=[illegible]
Date: Tue, 09 Nov 20...
```

cloud

Fig. 5. Search result for MongoDB with filter

The results of a single search resulted in, 867 IP addresses that are unsecure and using MongoDB. By selecting one of the IP addresses retrieved by the Shodan filtered search, more information can easily be obtained such as open ports, domains, ISP, and web technologies discovered on the result.



[redacted] Raw Data History

// TAGS: cloud

General Information

Hostnames	[redacted] azonaws.com
Domains	[redacted]
Cloud Provider	
Cloud Region	ap-northeast-1
Cloud Service	[redacted]
Country	[redacted]
City	
Organization	[redacted]
ISP	
ASN	AS16509

Open Ports

80

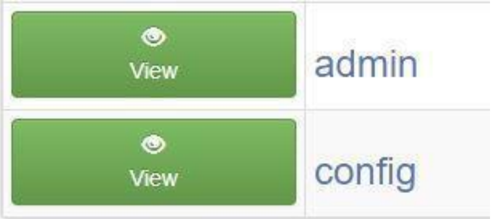
// 80 / TCP

Node.js

```
HTTP/1.1 200 OK
X-Powered-By: Express
Content-Type: text/html; charset=utf-8
Content-Length: 11760
ETag: [illegible]
Set-Cookie: mongo-express=[illegible]
Date: Tue, 09 Nov 2021 [illegible] GMT
Connection: keep-alive
Keep-Alive: timeout=5
```

Fig. 6. MongoDB Banner

Open databases like these are incredibly harmful to the security of an organization. Through one search, I was able to find a database susceptible to unauthorized examination. By pasting the IP address of the result, I was able to access a MongoDB database management webpage which allowed for the examination of some datasets contained within the page.



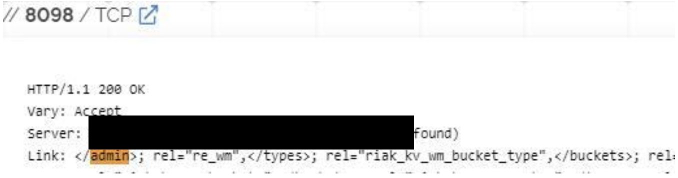
View	admin
View	config

Fig. 7. MongoDB Exposed Databases

Selecting the admin database would allow and outside observer to examine its contents which could result in the deletion or modification of files contained within the database

B. Discovering Riak vulnerabilities using Shodan

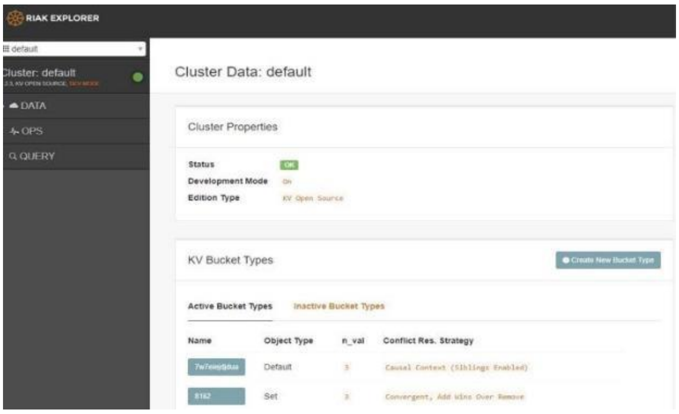
Common ports that belong to Riak include 8087, and 8089. Using a simple search filter "port:8087 riak", one can find numerous applications using Riak as a database. After selecting one of the results retrieved by Shodan, one can further examine the output information to see if any of the ports are directly connected to the Riak service and if it is connected to a webpage. In [Fig 8], while examining the 8098 port, it can be seen that a HTTP/ 1.1 200 OK request is returned. This information alerts that there is a HTTP page connected to this port. Furthermore, the link reference contains <admin>, meaning that this database possibly is allowing default admin access. When the IP of this result is typed into a URL followed by the 8098 port, it directs to a Riak explorer data page.



// 8098 / TCP

```
HTTP/1.1 200 OK
Vary: Accept
Server: [redacted] found)
Link: </admin>; rel="re_wm",</types>; rel="riak_kv_wm_bucket_type",</buckets>; rel
```

Fig. 8. Result examining Riak Result Found on Shodan



RIAK EXPLORER

default

Cluster: default

DATA

OPS

QUERY

Cluster Data: default

Cluster Properties

Status	OK
Development Mode	On
Edition Type	KV Open Source

KV Bucket Types

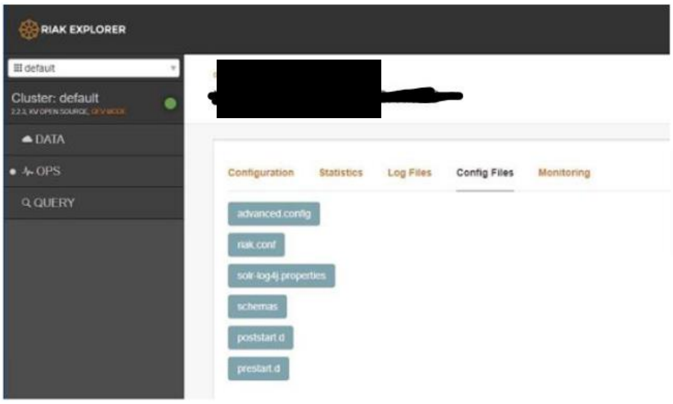
Create New Bucket Type

Active Bucket Types Inactive Bucket Types

Name	Object Type	n_val	Conflict Res. Strategy
7w7eiejtjdua	Default	3	Causal Context (Siblings Enabled)
8162	Set	3	Convergent, Add Wins Over Remove

Fig. 9. Riak Cluster Data

Further examination of unauthenticated database allows for one to examine resource usage metrics, Throughput metrics, and more. Individual nodes details can also be further examined. Node details include configuration information, configuration files, and log files. This information should always be secured, and it is apparent in a situation like this, that a security professional should be notified to mitigate this security vulnerability.



RIAK EXPLORER

default

Cluster: default

DATA

OPS

QUERY

[redacted]

Configuration Statistics Log Files Config Files Monitoring

advanced.config

riak.conf

solr-log4j.properties

schemas

poststart.d

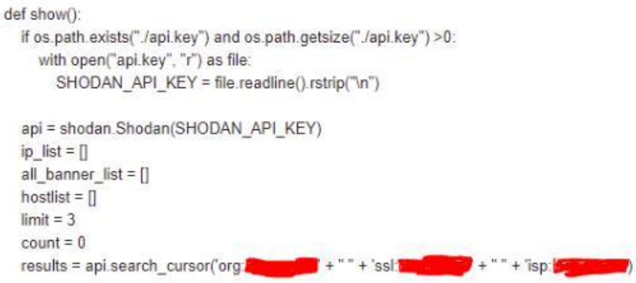
prestart.d

Fig. 9. Riak Cluster configuration

V. API USAGE FOR SECURITY

In the examples above it can be seen how Shodan has an extremely proficient ability at discovering security vulnerabilities contained in databases publicly connected to the internet. This ability is not just restrained to databases but can also be used to collect large amounts of data quickly and efficiently by using the Shodan API. The Shodan API allows for code to be written so that one may query Shodan and retrieve specified data. When one physically goes to the Shodan webpage, only a small number of results are provided. Even if a user purchases the enterprise version of Shodan, examining all the data collected will be incredibly tedious and inefficient. By purchasing the enterprise version of Shodan, one can query thousands of data entries quickly and output the data in numerous different ways. This is one of the main reasons why security professionals are starting to use Shodan more often. Security professionals will want to check if any of the devices or products from their business or organization are appearing on Shodan. If devices from one's organization does appear on Shodan, it would then be the job of the security professional to make sure that the information provided by Shodan does not show and security threats. Any threats discovered by Shodan would be an immediate security issue for the organization and could then be addressed with swiftly.

The benefit of the Shodan API is to easily obtain data that could be pertinent to an organization. There are numerous API calls one can make to retrieve data from Shodan. One of the easiest ways to collect bulk data for an organization would be using the Shodan API to grab banner information. As described earlier, banner information can include very useful information for security professionals. By creating a simple python script, I made the API search Shodan with a search filter to grab information from a specific organization that contained a certain SSL and ISP. Part of the code can be seen below in [Fig. 11].

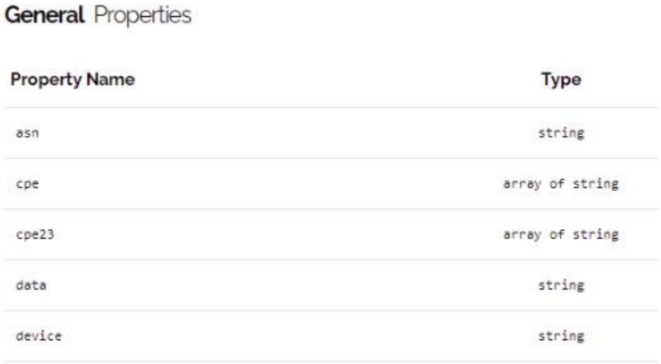


```
def show():
  if os.path.exists("./api.key") and os.path.getsize("./api.key") >0:
     with open("api.key", "r") as file:
        SHODAN_API_KEY = file.readline().rstrip("\n")

  api = shodan.Shodan(SHODAN_API_KEY)
  ip_list = []
  all_banner_list = []
  hostlist = []
  limit = 3
  count = 0
  results = api.search_cursor('org:[redacted]' + " " + 'ssl:[redacted] + " " + 'isp:[redacted])
```

Fig. 11. Shodan API Code

Although the limit of this API call is set to three, it would be common for a security professional to most likely use hundreds of API tokens at a time to scan depending on the size of the organization. Using the API can then be adjusted to grab banner information. Shodan has an extensive banner specification library that can be used to retrieve specific objects from the banner. Security professionals can use these banner filters to assist in the retrieval of wanted data. Cloud providers would most likely use more filters related to their needs, while other organizations could filter for specified open ports, products, or services. An example of some banner specifications for the API can be seen in [Fig.12].

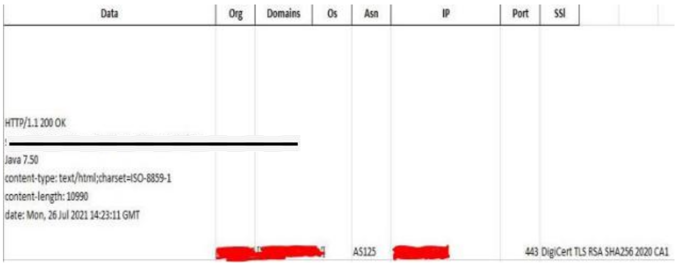


General Properties

Property Name	Type
asn	string
cpe	array of string
cpe23	array of string
data	string
device	string

Fig. 12. Shodan API Banner Filters

After running an API call containing search specifications and banner information, the results can be seen in [Fig.13]. This is a rather simple API call, however if an organization wanted to use Shodan to see if it had any products from its organization that were using a specific port, the API could reliably search through the Shodan database and find information that matched those parameters.



Data	Org	Domains	Os	Asn	IP	Port	Ssl
HTTP/1.1 200 OK [redacted] Java 7.50 content-type: text/html;charset=ISO-8859-1 content-length: 10990 date: Mon, 26 Jul 2021 14:23:11 GMT	[redacted]	[redacted]		AS125	[redacted]	443	DigiCert TLS RSA SHA256 2020 CA1

Fig. 13. API results

VI. Shodan Mitigation

As can be seen in the experiments above, Shodan can find a copious amount of information on devices connected to the internet. Using very simple methods, one can find numerous serious security vulnerabilities that can cripple the security of an organization very quickly. The idea that such a search engine exists can terrify businesses, but there are multiple ways one can try to mitigate vulnerabilities and Shodan's ability to discover devices. First, limiting devices to local networks will make them not visible on Shodan. Most databases and devices do not need to go publically online and should be set to share information only with other devices on the network. Another way one can decrease the amount of information Shodan receives from devices is to edit banner information to be as minimal as possible. Banners have the ability to be edited and unnecessary and valuable information should be removed to limit the amount of information Shodan gathers.

A simple way to mitigate unauthenticated connections would be to make sure all databases require usernames and passwords, and that these credentials are not the default credentials provided by the system. Shodan can search for services that have default credentials such as FTP. It is a best security practice to change credentials, and to have a strong password policy for services a nd databases. Another way that one can limit the capabilities of Shodan is to use a network firewall and create firewall rules to block Shodan scanners. Shodan uses an estimate of at least 16 different scanners to keep its indexing information updated. Blocking some of these known Shodan scanner IPs via firewall rules could assist and organization from having their devices discovered on Shodan.

VII. Conclusion

In this paper, vulnerabilities related to databases and API capabilities of Shodan was investigated. As a result of the investigation, it was shown that databases such as MongoDB and Riak can be incredibly susceptible to unauthorized access which can cause dire security issues for an organization. Shodan's API capabilities were also shown to be extremely effective and could greatly aide a security professional in gathering bulk data related to their organization or search parameters. Mitigation's techniques were then discussed for limiting the capabilities of Shodan and for securing database information. The effectiveness of Shodan to discover devices connected to the internet is very lucrative and can cause discomfort for many organizations. Due to the ever-growing evolution of the internet, better security practices must be met to reduce the amount of information provided by scanners, and to reduce the unauthorized access of databases.

References

[1] "Accessing unauthenticated mongodb database using shodan," Medium, 12-May 2020. [Online]. Available: https://greedybucks.medium.com/accessing-unauthenticated-mongodb-database-using-shodan-e62acc4a2922.

[2] A. Hansson, "Analyzing Internet-Connected Industrial Equipment."

[3] S. Lee, "Abnormal Behavior-Based Detection of Shodan and Censys-Like Scanning".

[4] T. Lee, "A Research on the Vulnerabilities of PLC using Search Engine.".

[5] "API documentation," Shodan. [Online]. Available: https://developer.shodan.io/api.

[6] D. Kirkpatrick, "Mongodb - security weaknesses in a typical nosql database," Trustwave, 21-Mar-2013. [Online]. Available: https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/mongodb-security-weaknesses-in-a-typical-nosql-databas e/.

[7] "Home Page," Riak. [Online]. Available: https://riak.com/index.html. [

[8] "How to block Shodan Scanners - the IPFIRE wiki," IPFire Wiki. [Online]. Available: https://wiki.ipfire.org/configuration/firewall/blockshodan.

[9] Matherly, "What is a banner?," Shodan Blog, 21-May-2020. [Online]. Available: https://blog.shodan.io/what-is-a-banner/.

[10] "KSEC snapshot - database disclosure," KSEC ARK - Pentesting and redteam knowledge base, 16-Dec-2019. [Online]. Available: https://www.ivoidwarranties.tech/posts/snapshots/databases/.

[11] P. Holescher, "How to remove your device from the shodan IOT search engine," Comparitech, 26-May-2021. [Online]. Available: https://www.comparitech.com/blog/vpn-privacy/remove-device-shodan/.

[12] R. Ho Published on: September 19, "What is shodan? how to use it & how to stay protected [2021]," Safety Detectives, 19-Sep-2021. [Online]. Available: https://www.safetydetectives.com/blog/what-is-shodan-and-how-to-use-it-most-effectively/. [

[13] "Shodan and python API," Alibaba Cloud Community. [Online]. Available: https://www.alibabacloud.com/blog/shodan-and-python-api_594919.