# Automating the Identification of Internet Resources for Healthcare Organizations using Shodan

By

Calvin Barreras

---

A Master's Paper Submitted to the Faculty of the

DEPARTMENT OF MANAGEMENT INFORMATION SYSTEMS

ELLER COLLEGE OF MANAGEMENT

In Partial Fulfillment of the Requirements

For the Degree of

MASTER OF SCIENCE

In the Graduate College

THE UNIVERSITY OF ARIZONA

2017

# STATEMENT BY AUTHOR

This paper has been submitted in partial fulfillment of requirements for an advanced degree at the University of Arizona.

Brief quotations from this paper are allowable without special permission, provided that an accurate acknowledgement of the source is made. Requests for permission for extended quotation from or reproduction of this manuscript in whole or in part must be obtained from the author.

SIGNED: Calvin L. Barreras

APPROVAL BY MASTERS PAPER ADVISOR

This paper has been approved on the date shown below:

_____ _____

Dr. Mark Patton Date

Lecturer of Management Information Systems

# ACKNOWLEDGEMENTS

I would like to thank my advisor, Dr. Mark Patton, for providing the knowledge and support I needed to finish this project. Without your guidance and optimism this project might never have been finished. To Dr. Hsinchun Chen, thank you for the opportunity to be a part of the Scholarship for Service program at the University of Arizona.

Additionally, I would like to thank my SFS compatriots, Cyrus Afarin, Vincent Ercolani, Rodney Rohrmann, John Grisham, Ashley Ireson, and Malaka El for making the last two years memorable. I wish you all the best of luck in life!

Most importantly I would like to thank my wife and children for supporting me as I worked through this project and the last six years of schooling. You are what motivates me to be a better person each and every day. Thank you from the bottom of my heart.

# Table of Contents

# List of Tables, Figures and Code Examples

# 1 Introduction

Organizations are under attack in today's digital environment (Symantec, 2017) and it is important to protect the assets that allow them to do their business. Hospitals, specifically, are a major target for hackers. Over 12 million medical records were compromised in 2016 alone. Medical device hijacking increased by 300% over the last three years and ransomware attacks specifically targeted hospitals (Savage & Coogan, 2015; Sheridan, 2016).

Hackers are targeting hospitals for several reasons. The primary reason is that data stolen from the healthcare industry, including both personal identifiable information and medical history information, cannot be recovered by changing a PIN or issuing a new card like what happens with financial data (Mearian, 2016). Additionally, the healthcare industry is an easy target because facilities often prioritize investments in life-saving equipment rather than in IT and security infrastructure (NetStandard, 2016).

To protect the healthcare assets that are being targeted, it is important to identify what devices the hackers might attack. The public-facing IP addresses an organization uses are often all a hacker needs to begin efforts to compromise systems. By focusing on these IP addresses, a hacker can gain knowledge of the operating systems, software versions, and open ports which might be vulnerable to exploits.

Shodan, a search engine for internet connected devices, provides a significant amount of this information. The gathering of Open Source Intelligence (OSINT), of which Shodan is a part of, is often required to look at how an organization deploys and identifies its internet presence. The threat of being hacked is great enough for healthcare facilities to go to great lengths to protect their internet presence.

# 2 Literature Review

Before investing time and resources into this project, a thorough review of domain specific research and literature was required. The scope of this project was focused on research in the domains of identifying internet resources and cyber-attacks on hospitals.

## 2.1 Identifying Internet Resources

| Paper | Focus | Methods | Data Source | Results |
|---|---|---|---|---|
| **Nikkel (2004)** | Digital Forensics | Command line utilities | Scanning Websites | Forensic evidence indicating domain ownership |
| **Markowsky & Markowsky (2015)** | Scanning IoT Devices | Combining Shodan queries with command line utilities | Shodan and scanning utilities | Vulnerable devices and servers affected by Heartbleed |
| **Matherly (2016)** | Banner search engine | IPv4 Internet scans | Shodan Module scans | Publicly accessible IP addresses, open ports, software versions, etc. |

*Table 1 - Literature for Identifying Internet Resources*

### *2.1.1 Key Findings*

Unix-style command line utilities and the tools built from them are still predominant in today's forensic environments. Nikkel's work to detail use of basic tools to investigate an Internet (http://www...) presence is still quite valid as the internet's (TCP/IP, networking, routing, etc.) underlying structure hasn't changed much in the last two decades. Of the command line scanning utilities that Markowsky explored – Nmap, Zmap, Masscan – the most stable application for scanning for open ports is Nmap (Jicha, Patton, & Chen, 2016). What is distinctive about Markowsky's work is that the Shodan search engine was used in conjunction with other tools to identify specific vulnerable devices.

The search engine for internet-connected devices, Shodan, provides a wealth of information. The Shodan website and API provide access to data gathered by scanning modules programmed to test for 234 specific open ports and services across the IPv4 address space (Jicha et al., 2016). The scanning modules collect data using an internally developed port scanner (not Nmap or Zmap as some might think). The information returned by the banner of the scanned devices is parsed and stored for retrieval through the website and API (Miessler, 2014).

The searchable information includes IP address, hostname, ISP, location, and device information (device type, software version, assigned port, etc.). Evaluating the Shodan scan information, an organization can validate its internet presence and test for unwanted configurations or software

versions that need updated. Conversely, a hacker can gather intelligence required to launch attacks.

## 2.2 Cyber Attacks

| Paper | Focus | Methods | Data Source | Results |
|---|---|---|---|---|
| **Savage & Coogan (2015)** | Ransomware | Data analysis | Ransomware data from Symantec | Ransomware is a prevalent threat |
| **Sheridan (2016)** | Healthcare attacks | Data summarization | Health and Human Services Breach Data | Healthcare industry experienced a 63% increase in attacks |
| **Walters (2016)** | Cyber-attacks | Data summarization | Compiled list of reported 2016 cyber-attacks | The private sector is lacking in its ability to defend their networks |
| **Symantec (2017)** | Internet Security | Cyber-attack analysis | Cyber-attack data from Symantec | Cyber-attacks have increased drastically over the last few years |

*Table 2 - Literature for Cyber Attacks*

### *2.2.1 Key Findings*

The incident rate and cost of major breaches in the healthcare industry is increasing according to all reviewed literature (Savage & Coogan, 2015; Sheridan, 2016; Walters, 2016; Symantec, 2017). In 2015, the average cost to the healthcare organization per stolen record was $398. The average global cost across all industries was $217. 2016 numbers were better, $355 and $158 respectively, but the difference was still significant. (HealthIT Security, 2016).

The increased incident rate of major breaches is likely due to what data is kept by medical institutions. A hospital record, for example, contains a name, birth date, demographic information such as address and phone number, emergency contacts, diagnoses, billing information, and possibly a social security number.

There are several illegal activities that can be facilitated with this information: identity theft, filing of false medical claims to purchase medical equipment or prescription drugs, use of "clean" diagnostic results to pass medical exams, filing of fake tax returns, and even extortion.

Hackers can sell this data for $60 or more on the black market compared to the $15 a social security number will yield or even less for credit card information (Akpan, 2016; NetStandard, 2016).

As a result of data breaches, healthcare organizations incur costs associated with data forensics, notifying involved parties, lawsuits, loss of business and brand value, and various other fines and penalties (Protenus, 2016). With such significant costs for the healthcare industry, the challenge is to balance a focus on saving lives and regulatory compliance with protecting the assets and data critical to their organization.

## 2.3 Research Gaps

Outside of what is being investigated at the University of Arizona, there appears to be few research efforts aimed at identifying medical devices on the internet. The literature reviewed demonstrates two facts: the healthcare industry is a major target for hackers and there are tools available to detect an organization's internet presence which are effective intelligence sources for the organization and hackers alike.

Though the cost of data breaches has declined from 2015 to 2016, the healthcare industry in the United States endures the highest cost per record compared to all industries globally. These disproportionate costs ultimately are passed on to the consumers of services and employees at healthcare facilities by way of increased insurance premiums, higher costs, or lower or stagnating compensation for healthcare workers (NetStandard, 2016).

Hackers are incentivized to steal healthcare information because it is often easier due to inadequate security measures and the payoff is substantial (Akpan, 2016). The likelihood of a breach increases proportional to the amount of medical information available. Legal requirements and government regulations exacerbate this as medical records are now largely in electronic format (Mearian, 2016).

Tools such as Shodan are excellent OSINT sources. They will be used to strengthen an organizations cybersecurity posture or to discover vulnerabilities and steal data. Hackers will

continue steal medical information until cybersecurity measures are adequate to deter them or it becomes less profitable.

Looking at the two facts demonstrated by the literature reviewed, an exploration in the use of the Shodan tool as an aid to researchers or healthcare organizations appears to be worth investigating.

### 2.4 Research Question

For this research, the focus is on identifying the entire span of public IPv4 addresses used by major medical groups or facilities which could be subject to identification and attack by a determined adversary. The initial search domain will use Shodan supplemented by traditional methods of looking up information about IP addresses such as nslookup (Name Server Lookup), DNS (Domain Name Services) queries, and WHOIS (Domain Name Registrar information). An effort to automate the process was explored.

The specific question being answered by this research is "Is it possible to identify the public internet IPv4 address spaces being employed by specific healthcare organizations?"

## 3 Methodology

### 3.1 Experiment Design

The goal of the experiment is to identify the specific IPv4 subnets being utilized by the organization with just the organization's name and website. To accomplish this, the Shodan API is queried and the results are analyzed. Command line tools such as nslookup and other online resources such as WHOIS tools can be used in addition to Shodan or to verify the results.

A successful iteration of the experiment is defined as adequately identifying the IPv4 subnets in use by the organization through automated methods (ex. "Fictitious Organization" with website www.404.com uses the IPv4 subnet(s) 192.168.14.0/24 and 10.25.0.0/16). A failed iteration is defined as an inability identify the organization's subnets through automatic and manual methods.

Note: This experiment is unlikely to expose every IPv4 subnet used by an organization in each instance of a successful iteration. The underlying facet of the Internet that allows an organization to identify their hosts is Domain Name Servers (DNS). DNS maintains a directory of domain names and their associated IP addresses so that a request to see the resources at www.example.com are routed to the appropriate IP address.

Additionally, the registration of domain names relies on information provided by people, which can be erroneous, incomplete, or obfuscated. WHOIS tools are used to provide this type of information.

For example, Banner Health, headquartered in Phoenix, AZ, acquired University Medical Center (UMC) and its facilities located in Tucson, AZ and Phoenix, AZ. Banner's existing IPv4 internet resources are easily identifiable in Shodan though none of the newly acquired internet resources associated with UMC facilities will be found.

### *3.1.1 Approach*

To address the question, the project is divided into two main sections. The first section involves identifying the healthcare organizations to analyze and their websites. The second section involves the automation effort and validation using command line utilities (Figure 1).

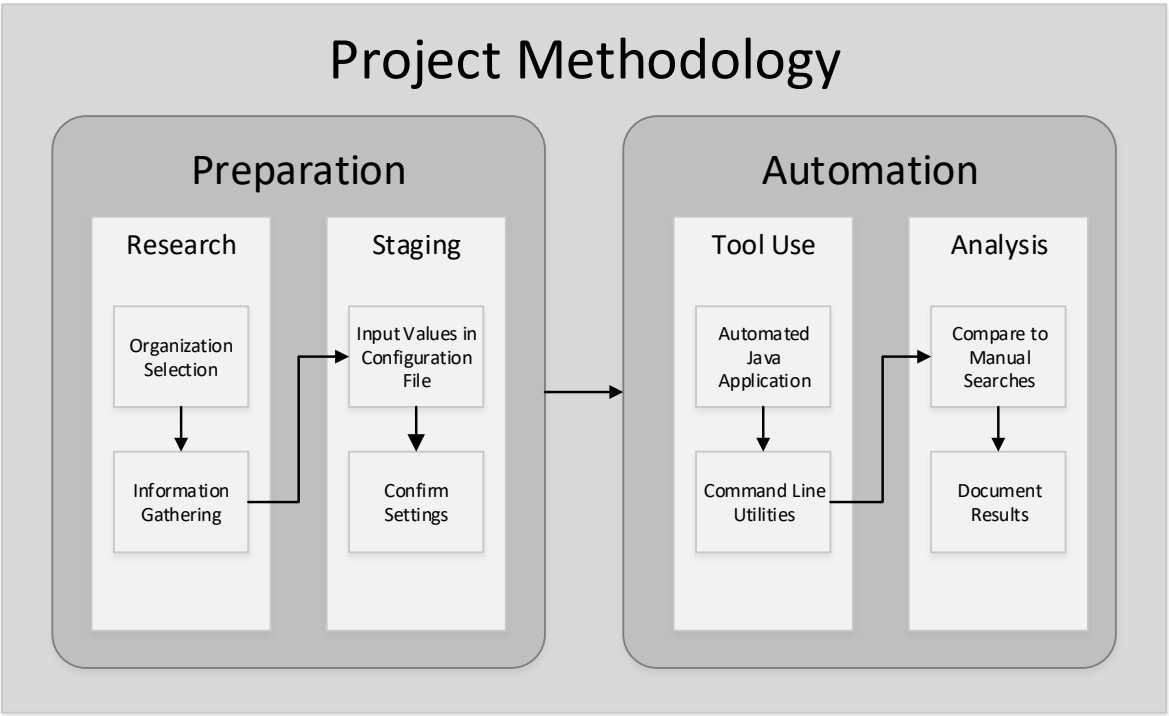


*Figure 1 - Project Methodology*

### *3.1.2 Organization Selection*

There are two resources that provide a wealth of information regarding healthcare facilities and systems. Both will be used to select major hospitals and the largest healthcare systems that operate multiple healthcare facilities (i.e. hospitals, clinics, emergency care facilities).

To identify individual hospitals to research, the American Hospital Directory (Ahd.com, 2017) was an invaluable resource. This website lists statistics about individual states and the major hospitals in each.

A second resource is used to identify the largest hospital systems in America (Bricker, 2016). Hospitals are often run by a larger organization (i.e. Banner Health, Kaiser Permanente, etc.) and this website provides basic statistics about the largest non-profit and for-profit hospital systems. Examples of the data provided by both resources can be found in Appendix A.

### *3.1.3 Tools*

The primary tool involved in this project is the Shodan API. The API allows highly customizable queries for internet-connected hosts that its scan modules have identified and catalogued. It is possible to search for hosts by IP address, port number, or numerous parameters that filter the data by geographic location, temporal delineation, IPv4 subnet, ISP, and bitcoin, HTTP, NTP, SSL, or telnet facets. The service functions by submitting a request to the Shodan API servers with the required elements. An example request URL for a host search is as follows:

```
https://api.shodan.io/shodan/host/search?key={YOUR_API_KEY}&query={query
}&facets={facets}
```

The service requires an account which provides the API_KEY. An example query for hosts used by the organization "Fictitious Organization" located in the United States follows:

```
https://api.shodan.io/shodan/host/search?key={YOUR_API_KEY}&query=org:"F
ictitious Organization"&country:"USA"
```

When a properly formatted request is submitted, Shodan returns a JSON (JavaScript Object Notation) array of matches. The JSON object is parsed easily for analysis.

In addition to the Shodan API, the command line utility nslookup is used to request the IPv4 address that is associated with an internet address (i.e. shodan.io resolves to 104.25.90.97). Other useful tools used in identifying internet resources in use by an organization are WHOIS lookup tools that return the registration information for an internet resource.

To automate this project, a program was written in Java to query the Shodan API, perform basic nslookup functions, and analyze the results. The Java application has helper methods that facilitate the automation:

- ShodanTools contains functions that interact with the Shodan API
- ShodanEntry is an object class allowing a query result to be manipulated
- ParseCSV provides functions for reading the tuples from the orgs.csv file
- ParseJSON contains functions to parse the JSON objects from a Shodan query
- DNSTools provides functionality similar to the command line utility nslookup
- DBTools provides a framework for interacting with database backends

- Analyzer provides functionality to determine IPv4 subnets and determine success

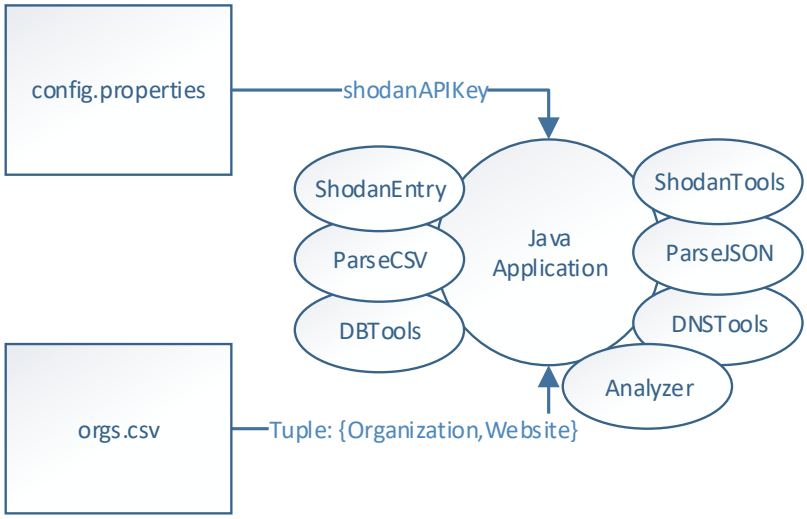


*Figure 2 - Diagram for Java Application*

The config.properties file contains such information as the Shodan API key unique to each account as well as database connection information. The orgs.csv file contains comma separated values for each organization, the organization name and its website.

### *3.1.4 Successful Use Case*

The first example is a successful search for the IPv4 address subnets used by the University of Arizona. In this example, and in all successful cases, two methods in ShodanTools are used to query Shodan. The first search method submits a query for an organization name. The second search method submits a query for an IP address subnet. Both searches are required to identify the internet presence of the organization and validate the results.

The Shodan search method employed performs a GET request through the REST API used to access Shodan data. The generic search string used in the Java application is:

```
"https://api.shodan.io/shodan/host/search?key=" + shodanAPIKey +
"&query=\"" + string + "\"&page=" + page
```

The `shodanAPIKey` variable is passed into the application from the config file that is setup to manage the application environment. The `string` variable that is passed into the query will

contain the necessary formatting to perform the correct search of Shodan (org:"{Organization Name}" or net:"{IPv4 subnet}"). The `page` variable is used to manage queries that return multiple pages and ensures that all results are analyzed.

For example, if querying for information about the University of Arizona, the organization name "University of Arizona" and website "www.arizona.edu" are pulled from orgs.csv file. The Shodan API key is loaded and the following query would be sent to Shodan:

```
https://api.shodan.io/shodan/host/search?key=<Shodan_API_Key>&query=org:
"University of Arizona"?&page=1
```

The results returned by the above search would be parsed and it is discovered that more than 6,000 IP addresses are associated with the University of Arizona. After paging through the complete list and capturing each IP address, specific IPv4 subnets are identified. In this case, the subnets for the University of Arizona are 128.196.0.0/16 and 150.135.0.0/16.

Though a subnet was identified for the University of Arizona by searching for the organization name, the website is evaluated as well. This step involves extracting the domain name from the organization's website address. In the case of http://www.arizona.edu, the domain name is arizona.edu. The IP address associated with the domain is resolved to an IP address (Code Example 1):

```
Record[] records = null;
        try {
                records = new Lookup("arizona.edu", Type.NS).run();
        } catch (TextParseException e) {
                e.printStackTrace();
        }
        for (int i = 0; i < records.length; i++) {
                NSRecord ns = (NSRecord) records[i];
                System.out.println("Host " + ns.getName() + " is
        managed by " + ns.getTarget());
                }
```

*Code Example 1 - DNS Code Snippet to Identify Name Servers*

This code performs a type NS (Name Server) lookup for the domain “arizona.edu”. The code iterates over the results and prints out all name servers associated with the domain. The resulting output is listed below:

```
Host arizona.edu. is managed by maggie.telcom.arizona.edu.
Host arizona.edu. is managed by penny.uits.arizona.edu.
Host arizona.edu. is managed by ns-remote.arizona.edu.
Host arizona.edu. is managed by optima.cs.arizona.edu.
Host arizona.edu. is managed by pendragon.cs.purdue.edu.
```

The first domain name server listed is the primary name server and can be used to query for the actual IP addressed used by the arizona.edu domain (Code Example 2).

```
resolver = new SimpleResolver("maggie.telcom.arizona.edu");
Lookup lookup = new Lookup("arizona.edu", Type.A);
lookup.setResolver(resolver);
Record[] records = lookup.run();
InetAddress address = ((ARecord) records[0]).getAddress();
System.out.println(address.getHostAddress());
```

*Code Example 2 - DNS Code to Perform Authoritative Name Server Lookup*

The above code outputs the IP address assigned to the domain arizona.edu:

```
128.196.128.233
```

The result is within the subnets identified previously. The process would be repeated for the mail server responsible for the domain arizona.edu. The code is similar to the examples above.

The overall result of this single query for the organization “University of Arizona” with a public website of “http://www.arizona.edu” is a return of the subnets 128.196.0.0/16 and 150.135.0.0/16. The results can be compared to Shodan API queries of each subnet. If the organization for each entry is the University of Arizona then one can assume that Shodan has successfully scanned and catalogued the IP address range in use by the university.

Validation of the Name Server lookups can be performed using the command line utility nslookup. To get the most accurate information, the DNS server responsible for managing the arizona.edu domain needs to be identified. The appropriate flags for such a search are shown in Figure 3 below.

```
C:\Users\cbarreras>nslookup -type=soa arizona.edu
Server:  UnKnown
Address:  192.168.1.1

Non-authoritative answer:
arizona.edu
        primary name server = maggie.telcom.arizona.edu
        responsible mail addr = hostmaster.arizona.edu
        serial  = 2017050406
        refresh = 7200 (2 hours)
        retry   = 3600 (1 hour)
        expire  = 86400 (1 day)
        default TTL = 7200 (2 hours)
```

*Figure 3 - Example nslookup to Identify Authoritative Name Server*

After identifying the appropriate name servers for the domain, the following nslookup query will return the required information:

```
C:\Users\cbarreras>nslookup arizona.edu maggie.telcom.arizona.edu
Server:  maggie.Telcom.Arizona.EDU
Address:  128.196.128.233

Name:    arizona.edu
Address:  128.196.128.233
```

*Figure 4 - Example nslookup to Obtain Correct IP Address*

The manual approach concurs with and validates the automatic approach.

### *3.1.5 Unsuccessful Use Case*

The automatic approach combined with manual tools for verification was not always successful. Following the same steps listed above, many queries ended in a maze of obfuscated IP addresses and ownership.

Organizations often mask their presence by way of third party companies who provide such services. Domain name registration through major hosting services like GoDaddy or Network Solutions. Domain proxy services are available as well. There are companies that will act as an organization's agent and forward requests and issues directly to them, protecting their anonymity.

Ascension Health is one of the largest non-profit hospital systems in the United States, operating 141 hospitals. Their website is “http://ascension.org/”. A Shodan query for the organization returns two IP addresses. A query for the name server responsible for ascension.org returns in IP address of 160.109.21.169. A Shodan query for the containing subnet 160.109.21.0/24 returns a list of IP addresses operated by Dell Services.

Digging deeper and looking at a WHOIS query for the domain, no name server is listed and the registration of the domain is handled through Network Solutions. The listed name servers, `NS1.ASCENSIONHEALTH.ORG` through `NS4.ASCENSIONHEALTH.ORG` all resolve to the sane 160.109.21.0/24 subnet.

This is a case where the organization is using a colocation facility (Dell Services) and Network Solutions to obfuscate their internet presence.

# 4 Conclusion

## 4.1 Results Summary

To validate the process described in this project, the top 10 non-profit hospital systems, representing over 300 hospitals across the United States, were analyzed. The results are summarized below (Table 3) and in more detail in Appendix B. The table columns indicate hospital system, number of subnets identified through Shodan, whether the iteration proved successful as noted in section 3.1, and comments.

| Hospital | Subnets | Success | Comment |
|---|---|---|---|
| **Ascension Health** | 1 | No | Obfuscated |
| **Trinity Health** | 0 | No | Obfuscated, DNS IP points to Trinity Information Services, Website IP points to MEDSEEK |
| **Kaiser Permanente** | 1 | No | Numerous organizations listed in Shodan |
| **Dignity Health** | 9 | Yes | 3rd party DNS |
| **Catholic Health Initiatives** | 4 | Yes | 3rd party Website Hosting/Registration |
| **Adventist Health System** | 9 | Yes | |
| **Sutter Health** | 3 | Yes | 3rd party Website Hosting/Registration |
| **Providence Health & Services** | 5 | Yes | |
| **Banner Health** | 7 | Yes | 3rd party DNS |
| **Baylor Scott & White Health** | 5 | Yes | |

*Table 3 - Summary of Experiment Results*

These results indicate that only the two largest non-profit hospital systems have taken measures to hide their internet presence. The third largest, Kaiser Permanente, is benefiting from multiple organizations with the word "Kaiser" in their organization name. Manual searching of Shodan still yields some subnet information for the hospital system. Of the remaining seven, two are using a 3rd party DNS service and two are using 3rd party website hosting/registration.

Ascension Health appeared to have nearly their entire public presence hosted by a 3rd party, Dell Services. This choice provides many benefits, namely full utilization of hardware due to shared

server infrastructure, lower power costs, lower staffing costs, zero capital costs, and resilience without redundancy (Jennings, 2017).

Trinity Health and Kaiser Permanente appear to rely on security through obscurity, or the belief that their systems will be secure so long as nobody outside of their organizations can find them. This practice alone is a weak security measure, but layered on top of good security measures, security through obscurity can be a strong addition to an overall security posture (Miessler, 2009).

The remaining hospital systems use IPv4 subnets that are easily identifiable. This means that their publicly facing hosts are easy to find by concerned parties within and without their organizations. That could mean that they are more likely to be targeted by hackers. Of these hospitals, the only organization with a major breach was Banner Health.

## 4.2 Reflection

The experiment provided valuable insight into answering the question, “Is it possible to identify the internet resources employed by specific healthcare organizations?” In a lot of cases, the attempt to provide the requested data was a success. Given an organization name and its website address, it was possible to return the specific IP address subnets used. In cases where organizations tried to hide their internet presence, more sophisticated methods would be required to identify their specific internet resources.

This was a fun exercise to test the efficacy of the Shodan API and to use command line utilities for this use. There is a lot of room to take research like this and it is my hope that the methods discussed in this paper will prove valuable to other research efforts.

## 4.2 Future Directions

The bane of many efforts like this is a heavy reliance on knowledge of command line utilities and a programming language. If this work were to be continued, development of a GUI and a database backend would be crucial. A tool that is easy to configure and use and able to work with a variety of database flavors has the potential to save some research effort countless hours of time.

# REFERENCES


Ahd.com. (2017). American Hospital Directory - Hospital Statistics by State. Retrieved May 1, 2017, from https://www.ahd.com/state_statistics.html

Akpan, N. (2016). Has health care hacking become an epidemic? | PBS NewsHour. Retrieved May 6, 2017, from http://www.pbs.org/newshour/updates/has-health-care-hacking-become-an-epidemic/

Bricker, E. (2016). Top 30 Largest Hospital Systems in America. Retrieved May 5, 2017, from http://www.compassphs.com/blog/healthcare-trends/healthcare-fast-facts-top-30-largest-hospital-systems-in-america/

HealthIT Security. (2016). Healthcare Data Breach Costs Still Highest Among Industries. Retrieved May 6, 2017, from http://healthitsecurity.com/news/healthcare-data-breach-costs-still-highest-among-industries

Jennings, R. (2017). 5 Financial Benefits of Moving to the Cloud. Retrieved May 9, 2017, from https://www.webroot.com/us/en/business/resources/articles/cloud-computing/five-financial-benefits-of-moving-to-the-cloud

Jicha, R., Patton, M. W., & Chen, H. (2016). Identifying Devices Across the IPv4 Address Space. In *IEEE Conference on Intelligence and Security Informatics (ISI)* (pp. 199–201). Tucson, AZ. https://doi.org/10.1109/ISI.2016.7745469

Markowsky, L., & Markowsky, G. (2015). Scanning for vulnerable devices in the Internet of Things. In *2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)* (Vol. 53, pp. 463–467). IEEE. https://doi.org/10.1109/IDAACS.2015.7340779

Matherly, J. (2016). Shodan Developer. Retrieved May 1, 2017, from https://developer.shodan.io/api

Mearian, L. (2016). Hackers are coming for your healthcare records -- here's why | Computerworld. Retrieved May 1, 2017, from http://www.computerworld.com/article/3090566/healthcare-it/hackers-are-coming-for-your-healthcare-records-heres-why.html

Miessler, D. (2009). Obscurity is a Valid Security Layer. Retrieved May 8, 2017, from https://danielmiessler.com/study/security-by-obscurity/

Miessler, D. (2014). A Shodan Tutorial and Primer. Retrieved May 7, 2017, from https://danielmiessler.com/study/shodan/

NetStandard. (2016). Why Hackers Want Your Medical Records | NetStandard Managed IT. Retrieved May 1, 2017, from http://www.netstandard.com/hackers-want-medical-records/

Nikkel, B. J. (2004). Domain name forensics: a systematic approach to investigating an internet presence. *Digital Investigation*, *1*(4), 247–255. https://doi.org/https://doi.org/10.1016/j.diin.2004.10.001

Protenus. (2016). Bringing the Cost of Healthcare Data Breaches Into Focus. Retrieved May 1, 2017, from https://www.protenus.com/blog/cost-of-healthcare-data-breaches

Savage, K., & Coogan, P. (2015). *The evolution of ransomware*. *Security Response* (Vol. 1). Retrieved from http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-evolution-of-ransomware.pdf

Sheridan, K. (2016). Major Cyberattacks On Healthcare Grew 63% In 2016. Retrieved May 2, 2017, from http://www.darkreading.com/attacks-breaches/major-cyberattacks-on-healthcare-grew-63--in-2016/d/d-id/1327779

Symantec. (2017). *Internet Security Threat Report*. Retrieved from https://www.symantec.com/security-center/threat-report

Walters, R. (2016). Cyber Attacks on U.S. Companies in 2016. *The Heritage Foundation: Issue Brief*, *No. 4636*(December), 1–5. Retrieved from http://www.heritage.org/defense/report/cyber-attacks-us-companies-2016

# APPENDIX A – Hospital Statistics

Truncated list of hospital statistics by state (retrieved from American Hospital Directory, https://www.ahd.com/state_statistics.html)

Statistics for non-federal, short-term, acute care hospitals are summarized by state.

Data are based on each hospital's most recent Medicare cost report.

| State | Number Hospitals | Staffed Beds | Total Discharges | Patient Days | Gross Patient Revenue ($000) |
|---|---|---|---|---|---|
| AK - Alaska | 11 | 1,203 | 44,445 | 226,475 | $4,095,303 |
| AL - Alabama | 93 | 15,725 | 573,853 | 2,818,342 | $50,305,462 |
| AR - Arkansas | 50 | 7,940 | 319,173 | 1,394,034 | $21,974,629 |
| AS - American Samoa | 1 | 0 | 0 | 0 | $0 |
| AZ - Arizona | 73 | 13,715 | 680,304 | 2,634,274 | $60,642,839 |
| CA - California | 345 | 74,806 | 3,115,787 | 14,316,135 | $357,873,341 |
| CO - Colorado | 53 | 8,518 | 383,773 | 1,712,147 | $49,315,780 |
| CT - Connecticut | 34 | 9,213 | 377,950 | 1,794,782 | $33,850,270 |
| DC - Washington D.C. | 8 | 2,603 | 105,119 | 608,659 | $10,537,559 |
| DE - Delaware | 8 | 2,014 | 88,651 | 439,615 | $6,375,064 |
| FL - Florida | 218 | 54,674 | 2,461,784 | 11,840,030 | $252,656,650 |
| GA - Georgia | 114 | 22,160 | 887,912 | 4,419,387 | $81,385,608 |
| GU - Guam | 3 | 201 | 9,488 | 49,071 | $159,368 |
| HI - Hawaii | 14 | 2,505 | 92,402 | 523,778 | $6,289,634 |
| IA - Iowa | 40 | 6,423 | 272,290 | 1,186,603 | $20,443,269 |
| ID - Idaho | 17 | 2,398 | 111,748 | 452,006 | $9,034,905 |
| IL - Illinois | 142 | 30,368 | 1,277,020 | 5,757,206 | $125,370,683 |
| IN - Indiana | 98 | 15,977 | 670,408 | 3,063,127 | $62,908,771 |
| KS - Kansas | 59 | 6,362 | 264,178 | 1,142,609 | $25,454,336 |
| KY - Kentucky | 76 | 13,976 | 544,376 | 2,638,378 | $46,477,278 |
| LA - Louisiana | 105 | 14,985 | 496,707 | 2,381,725 | $44,062,738 |
| MA - Massachusetts | 78 | 15,553 | 749,427 | 3,558,399 | $55,254,875 |
| MD - Maryland | 52 | 11,100 | 589,989 | 2,922,215 | $18,115,336 |
| ME - Maine | 21 | 3,112 | 117,889 | 547,891 | $9,086,557 |
| MI - Michigan | 105 | 23,486 | 1,100,851 | 4,882,527 | $77,949,041 |
| MN - Minnesota | 56 | 10,503 | 465,799 | 2,080,233 | $36,575,652 |
| MO - Missouri | 88 | 16,845 | 680,483 | 3,170,955 | $60,782,793 |
| MP - Northern Mariana Islands | 1 | 74 | 3,027 | 17,399 | $0 |
| MS - Mississippi | 70 | 10,707 | 331,251 | 1,585,760 | $28,585,813 |

List of Top 30 Largest Hospital Systems in America (retrieved from Compass Professional Health Services Blog, http://www.compassphs.com/blog/healthcare-trends/healthcare-fast-facts-top-30-largest-hospital-systems-in-america/)

List format: Hospital Facility/Organization (Headquarter City) – Number of hospitals

## Non-Profit Hospital Systems

1. Ascension Health (St. Louis) – 76
2. Trinity Health (Livonia, Mich.) – 45
3. Kaiser Permanente (Oakland, Calif.) – 37
4. Dignity Health (San Francisco) – 36
5. Catholic Health Initiatives (Englewood, Colo.) – 33
6. Adventist Health System (Winter Park, Fla.) – 31
7. Sutter Health (Sacramento, Calif.) – 26
8. Providence Health and Services (Renton, Wash.) – 26
9. Banner Health (Phoenix) – 20
10. Baylor Scott & White Health (Dallas) – 19
11. CHRISTUS Health (Irving, Texas) – 19
12. SSM Health Care (St. Louis) – 18
13. Intermountain Health Care (Salt Lake City) – 17
14. Mercy Health (Cincinnati) – 17
15. NewYork-Presbyterian Healthcare System (New York City) – 17
16. Adventist Health (Roseville, Calif.) – 16
17. UPMC (Pittsburgh) – 16
18. North Shore-Long Island Jewish Health System (Great Neck, N.Y.) – 15
19. UnityPoint Health (Des Moines, Iowa) – 15
20. Hospital Sisters Health System (Springfield, Ill.) – 14
21. Mercy (Chesterfield, Mo.) – 14
22. Texas Health Resources (Arlington) – 14
23. Aurora Health Care (Milwaukee) – 13
24. Baptist Memorial Health Care (Memphis, Tenn.) – 13
25. Franciscan Alliance (Mishawaka, Ind.) – 13
26. Saint Joseph Health (Orange, Calif.) – 13
27. Carolinas HealthCare System (Charlotte, N.C.) – 12
28. Bon Secours Health System (Marriottsville, Md.) – 11
29. Mayo Clinic Health System (Rochester, Minn.) – 11
30. Sentara Healthcare (Norfolk, Va.) – 12
31. Novant Health (Winston-Salem, N.C.) – 10
32. East Texas Medical Center Regional Healthcare System (Tyler) – 7

## For-Profit Hospital Systems

1. Community Health Systems –188 s
2. Hospital Corporation of America (HCA) – 166
3. Tenet Healthcare (Dallas) – 74
4. LifePoint Health (Brentwood, Tenn.) – 56
5. Prime Healthcare Services (Ontario, Calif.) – 32
6. Universal Health Services (King of Prussia, Pa.) – 28
7. IASIS Healthcare (Franklin, Tenn.) – 18
8. Ardent Health Services (Nashville, Tenn.) – 12
9. Capella Healthcare (Franklin, Tenn.) – 9
10. Steward Health Care System (Boston) – 9
11. National Surgical Hospitals (Chicago) – 8

# APPENDIX B – Results

| Organization | Website | Domain | Domain IP | Name Server | Name Server IP |
|---|---|---|---|---|---|
| Ascension Health | http://www.ascension.org | ascension.org | 160.109.21.169 | ns3.ascensionhealth.org | 160.109.21.109 |
| Trinity Health | http://www.trinity-health.org/ | trinity-health.org | 199.117.41.89 | ns1.trinity-health.org | 170.232.224.9 |
| Kaiser Permanente | https://healthy.kaiserpermanente.org/ | kaiserpermanente.org | 162.119.200.164, 162.119.192.164 | ea-dns14.kp.org | 162.119.132.55 |
| Dignity Health | https://www.dignityhealth.org/ | dignityhealth.org | 162.135.7.134 | ns10.dnsmadeeasy.com | 208.94.148.4 |
| Catholic Health Initiatives | http://www.catholichealthinitiatives.org/ | catholichealthinitiatives.org | 52.165.39.95 | ns4.catholichealth.net | 199.34.6.18 |
| Adventist Health System | http://adventisthealthsystem.com/ | adventisthealthsystem.com | 204.139.85.176 | dns1.ahss.org | 204.139.85.10 |
| Sutter Health | http://www.sutterhealth.org/ | sutterhealth.org | 198.217.73.118 | ns1-05.azure-dns.com | 40.90.4.5 |
| Providence Health and Services | http://www.providence.org/ | providence.org | 173.203.24.150 | authns2.qwest.net | 208.44.130.120 |
| Banner Health | https://www.bannerhealth.com/ | bannerhealth.com | 206.213.44.79 | pdns01.domaincontrol.com | 216.69.185.50 |
| Baylor Scott & White Health | https://www.bswhealth.com/ | bswhealth.com | 198.205.24.58 | ns03.baylorhealthcare.com | 198.205.24.6 |

| Mail Server | Shodan Subnet(s) | Identified Subnet(s) | Success? | Note |
|---|---|---|---|---|
| dnsadmin.ascensionhealth.org | 12.109.79.252/31 | 1 | No | Obfuscated |
| webadmin.trinity-health.org | | | No | SOA query returns uthdchns05.trinity-health.org as primary name server, WHOIS provided name server |
| hostamaster.kp.org | 192.119.0.0/16 | 1 | No | SOA query returns ca5-dns.kp.org as primary name server, WHOIS provided name server, Shodan search for Kaiser returned several organizations |
| dns.dnsmadeeasy.com | 162.135.6.0/24, 162.135.7.0/24, 162.135.12.0/24, 162.135.4.0/24, 162.135.192.0/24, 206.132.94.130/32 | 9 | Yes | 3rd party DNS |
| dnsadmin.catholichealth.net | 199.34.4.0/24, 199.34.5.0/24, 199.34.6.0/24, 199.34.0.0/24 | 4 | Yes | Website hosted externally with Network Solutions |
| dnsadmin.ahss.org | 204.139.65.0/24, 204.139.67.0/24, 204.139.84.0/24, 204.139.85.0/24, 204.139.87.0/24, 204.139.88.0/24, 206.210.160.0/24, 206.210.162.0/24 | 9 | Yes | |
| admin | 198.217.72.0/24, 198.217.73.0/24, 198.217.74.0/24 | 3 | Yes | Website hosted externally with Microsoft Azure |
| orhostmaster.phsor.org | 69.238.162.0/24, 170.173.0.0/24, 170.173.2.0/24, 170.173.4.0/24, 170.173.16.0/24 | 5 | Yes | SOA query returns u6059.providence.org as primary name server |
| dns.jomax.net | 206.213.26.0/24, 206.213.27.0/24, 206.213.41.0/24, 206.213.43.0/24, 206.213.44.0/24, 206.213.62.0/24, 206.213.63.0/24, | 7 | Yes | 3rd party DNS |
| admin.baylorhealthcare.com | 198.205.16.0/24, 198.205.17.0/24, 198.205.19.0/24, 198.205.24.0/24, 199.119.25.0/24 | 5 | Yes | |