Does Shodan Keep Up With The Times?

By

Cyrus Afarin

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 thesis 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: Cyrus Afarin

APPROVAL BY MASTERS PAPER ADVISOR

This paper has been approved on the date shown below:

_____ 05/05/2017

Dr. Mark Patton Date

Lecturer of Management Information Systems

Table of Contents

LIST OF FIGURES

LIST OF TABLES

ABSTRACT

Through security visualizations, Shodan data can be utilized to understand SCADA and ICS devices for any given IP range. The relationship between ports and IP addresses can be displayed in a manner to obtain valuable information and to understand Shodan as a tool. An analysis of Shodan data will be performed over a specified period for a specific region. These efforts are framed to accurately identify SCADA/ICS devices for said region and understand Shodan's consistency over the evaluated time frame.

1 INTRODUCTION

The growth of internet-enabled devices continues in today's technology centered world. Additionally, security concerns over these internet-enabled devices that are used in personal, business, industrial, or enterprise environments has also evolved. Major concerns over critical infrastructure devices that control power, water, gas, and other key items within infrastructure have gained traction as researchers, security professionals, and adversaries are able to rapidly identify these devices on the internet. Vulnerabilities found within these types of systems or devices can be abused to cause damage, control resources, or even held accountable from a political standpoint. Identification of these devices must be performed through internet scanning and understanding the communication protocol and the information being shared is key to protecting these devices moving forward.

The ease of identification has been due to the increasing development and capabilities of the tool known as Shodan. This tool is owned and operated by John Matherly of the University of Michigan and is known to be able to scan and identify internet facing devices.

In order to understand Shodan as a tool over time and have the ability to identify what ICS devices are running on any given port a small-scale case study was proposed. The country of focus for this research is Venezuela due to its current political and economic climate as compromise of critical devices within the country would further its downfall. Daily dumps of Shodan data have been gathered by the University of Arizona, however this research focuses on the scan data from the entirety of August 2016 compared to the entirety of January 2017 for Venezuela. The motivation for this research is to understand if Shodan scans differ over time within the same region and to be able to identify Supervisory Control and Data Acquisition (SCADA) and Industrial Control System (ICS) devices in Venezuela.

2 BACKGROUND/LITERATURE REVIEW

2.1 Literature Review

2.1.1 Background Area 1 (SCADA Shodan devices)

Shodan, a search engine for the Internet of Things (IoT) can help provide a novel data source for CTI visualizations (Bodenheim, 2014). Due to the assumption that SHODAN indexes devices within 3 weeks of coming online, it was necessary to understand its role within SCADA and ICS devices specifically and Bodenheim explains that Shodan users can find indexed devices, including Supervisory Control and Data Acquisition devices (Bodenheim, 2014). Additionally, the use of TCP/IP protocols in modern SCADA systems has led to a heightened susceptibility to traditional exploits such as Operating System (OS) attacks and DDoS (Ayuburi et al., 2015; Onyeji et al., 2014). Trend Micro and the Organization of American States (OAS) have data that supports a rise in the number of attacks against critical infrastructure (Trend Micro, 2013). Therefore, it is

necessary to understand what protocols are being run on ICS/SCADA devices within Venezuela and if vulnerabilities are present.

2.1.2 Background Area 2 (Venezuela)

Due to the current political and societal posture of Venezuela, it has a need to be studied in terms of how cyber may also be effected from the turmoil. There is growing recognition of the extent of cyber criminality across Latin America. Additionally, there is growing preoccupation with hacktivist groups targeting official institutions and agencies with the intent of expressing political and social grievances (Diniz, et al., 2012). “More and more, malware will be homegrown and used against governments, the private sector and citizens” (Wharton, 2017). Despite the lack of specificity given towards Venezuela, clearly the threat landscape is growing in the surrounding region and cyber threat intelligence in some form or another is needed. Knowledge of the cyberthreat landscape and government responses in Latin America is weak. More specific data is needed to accurately diagnose the threat to our citizens (Trend Micro, 2013).

2.1.3 Background Area 3 (Security Visualizations)

Security data visualization is becoming extremely important due to big data, machine learning and exploratory data analytics. Due to the volume of data in big data it is extremely impossible to find anomalies using traditional methods (Balakrishnan, 2014). Very little work has been conducted around security visualizations that specifically address ICS/SCADA devices within the Shodan dataset. We focus on finding SCADA and ICS devices due to their critical role in infrastructure support (Ercolani, 2016). The research performed by Ercolani on visualizing Shodan was the introductory foundation taken to perform the research within this paper over time. Because the methodology for understanding Shodan data through visualizations by Ercolani was so effective, a similar approach will be taken to obtain accurate results. VisSec’s primary purpose is to assist

network security analysts in detecting, stopping, and defending against current and future network attacks (Attipoe, 2016). This literature reiterates the need for visualizations, and specifically towards industrial control systems due to their critical role in any country/society. Due to the large amounts of Shodan data, visualizations should be utilized for presenting the information in a easy to consume format.

2.1.4 Research Gaps

After the literature review over the previously mentioned background areas, a few research gaps were identified. Substantial studies on utilizing Shodan data are abundant however nothing has been done to analyze Shodan data over time for a specific area/region despite the claim that for each discovered service, Shodan scans and stores results repeatedly over time (Genge, 2015). Another gap identified was the lack of ICS device identification within Latin America (Venezuela specifically). Lastly, it is found that very few researchers are utilizing visualizations to represent the data from a security standpoint. Therefore, resourceful cyber posture analytics, especially in Latin America, is missing.

3 CASE STUDY/METHODOLOGY/CONTENT

3.1 Introduction

For the identification of ICS and SCADA devices in Venezuela, the Shodan data collected by the University of Arizona needed to be parsed and stored in a MySQL database. The data was queried based off August 2016 data and January 2017 data. These two months were chosen because all the scan data for the entirety of both months had been made available to the university. The data set being analyzed was gained through IP addresses identified as either ICS or SCADA considering

the Shodan module for that data point. The following sections describe the data storage, contents of the data, and analysis performed

3.2 Initial Data

This section discusses where the tables specifically for Venezuela were derived from. The process of table creation is presented and the details of the data are discussed for a better holistic view of the contents that were being used for the study.

3.2.1 Data Storage

Before being able to extract the ICS/SCADA device data for Venezuela and perform analysis many processing steps were to be performed. Parsing the Shodan data from its entirety into a MySQL database was initially required. This task was performed by Vincent Ercolani (another Master's student) due to his research involving much more of the Shodan data and having the skillset to handle the parsing and storing tasks. The parsing was performed through Python scripts and upload time onto the database server took 2 weeks. Once the entirety of the Shodan data was available, another database was created to specifically contain Venezuela data for August 2016 and January 2017. This data was queried from the original dataset based off the Shodan modules, IP address, ports, and protocol information and stored as separate tables within the subset database. Three separate tables were created per month. These tables separated ports, IP addresses, and the ICS

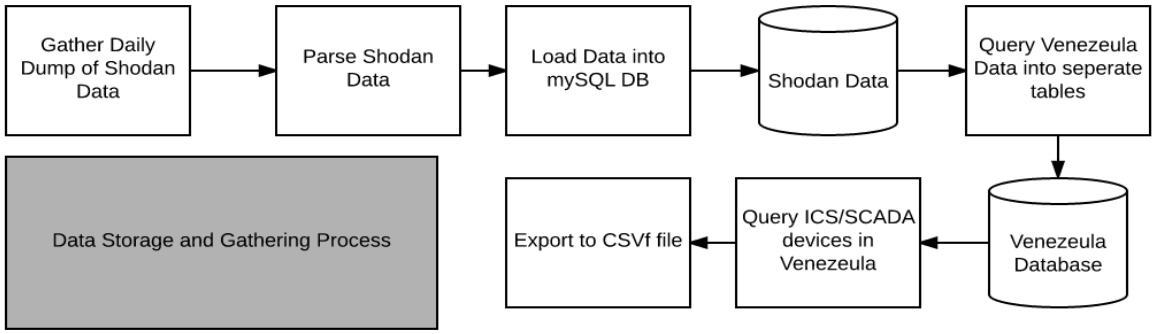

Figure 1 - Data Storage Process

relationships. Further details on the table contents will be discussed in sections to come. It should be noted that the data is only that of IP addresses that were known to contain ICS devices based off Shodan modules. The data collection and storage process can be seen in Figure 1 above.

3.2.2 Data Contents

In order to have the appropriate data for the analysis to take place it was necessary to gather the data around IP addresses and ports respectively. These files were extracted from the MySQL database to csv files. The data is separated into an IP node csv and port node csv. This was necessary for the analysis portion when trying to visualize the IP-port relationships. Additionally, there are IP node and port node csv files for August 2016 and January 2017. The IP node table contains the following data points:

- ID, Label (IP address), Organization owning the IP, Internet Service Provider (ISP), Type

The port node table contains the following data points:

- ID (port-protocol combo), Label, port, shodanModule, Type

One thing to note is that shodanModule and Type were defined within the entire Shodan dataset that this subset of data was queried from. Samples of the data files can be seen below with the information they each contain.

ID	Label	Org	ISP	Type
2892989699	172.111.133.3	Micfo, LLC.	Secure Internet LLC	IP
1759510531	104.224.0.3	Roya Hosting LLC	Roya Hosting LLC	IP
3131511251	186.167.17.211	Corporacion Digitel C.A.	Corporacion Digitel C.A.	IP
3126374574	186.88.176.174	CANTV	CANTV	IP
3361363126	200.90.84.182	CANTV	CANTV	IP
3190291588	190.39.252.132	CANTV	CANTV	IP
3198812699	190.170.2.27	Universidad del Zulia	Universidad del Zulia	IP
3190053610	190.36.90.234	CANTV	CANTV	IP
3201136221	190.205.118.93	CANTV	CANTV	IP

Table 1: IP node sample

ID	Label	Port	shodanModule	Type
8069http	8069 http	8069	http	HTTP
7657http	7657 http	7657	http	HTTP
1962pcworx	1962 pcworx	1962	pcworx	ICS
22ssh	22 ssh	22	ssh	Port
2222plc5	2222 plc5	2222	plc5	ICS
5009apple-airport-admin	5009 apple-airport-admin	5009	apple-airport-admin	Port
13579http	13579 http	13579	http	HTTP
11845hart-ip-udp	11845 hart-ip-udp	11845	hart-ip-udp	ICS
80http	80 http	80	http	HTTP

Table 2: Port / Shodan Module node sample

Lastly, from these two datasets an edge file needed to be created for the anaylsis phase. This csv file was merely a fusion of the IP node and port node table to include:

- Source (same as ID in IP), target (same as ID in node), port, shodanModule

This file is used as the edge points within the visualization portion of the study and was necessary to create the relationship between IP and port combinations. Edge files were again created for both August 2016 and January 2017.

3.3 Analysis Performed

This section presents the tool used for analysis, the steps involved to gain the insightful visualizations, and the actual results.

3.3.1 Process within Gephi

To utilize the datasets and understand the Shodan scans from a comparitive perspective, visualizations were performed through network graph analysis. The tool of choice for visualizing the data was Gephi. The following steps were taken in order to gain a visualization amongst the relationships:

- Import IP node csv and port node csv into the node table within Gephi
- Import the ICS relations csv as the edges table
- Run Force Atlas layout for visualization
- Change reputation strength to 2000 (provides better spread on data layout)
- Partition appearance on coloring

These steps were performed indepedently for coloring by modularity where we are able to see clusters of IP and port relationships. The other graph created was based off of type which is a less granulated category of the shodan modules (seen in the port node table). The type graph analysis separates IP addresses from the shodan modules themselves. Through this representation of the data we can compare what ICS/SCADA device IP addresses had what protocols running on them and then easily compare and contrast to the “same data” over a different time period (August vs January). Additionally, the graphs contained data points that were sized by the level of their degree. Average degree, graph density, and modularity were run on the visualization.

4 Results & Discussion

4.1 Results

This section goes over the visualizations developed and what details can be seen within the data itself. Within this section, results will be discussed and key findings will be showcased.

4.1.1 Type Visualizations

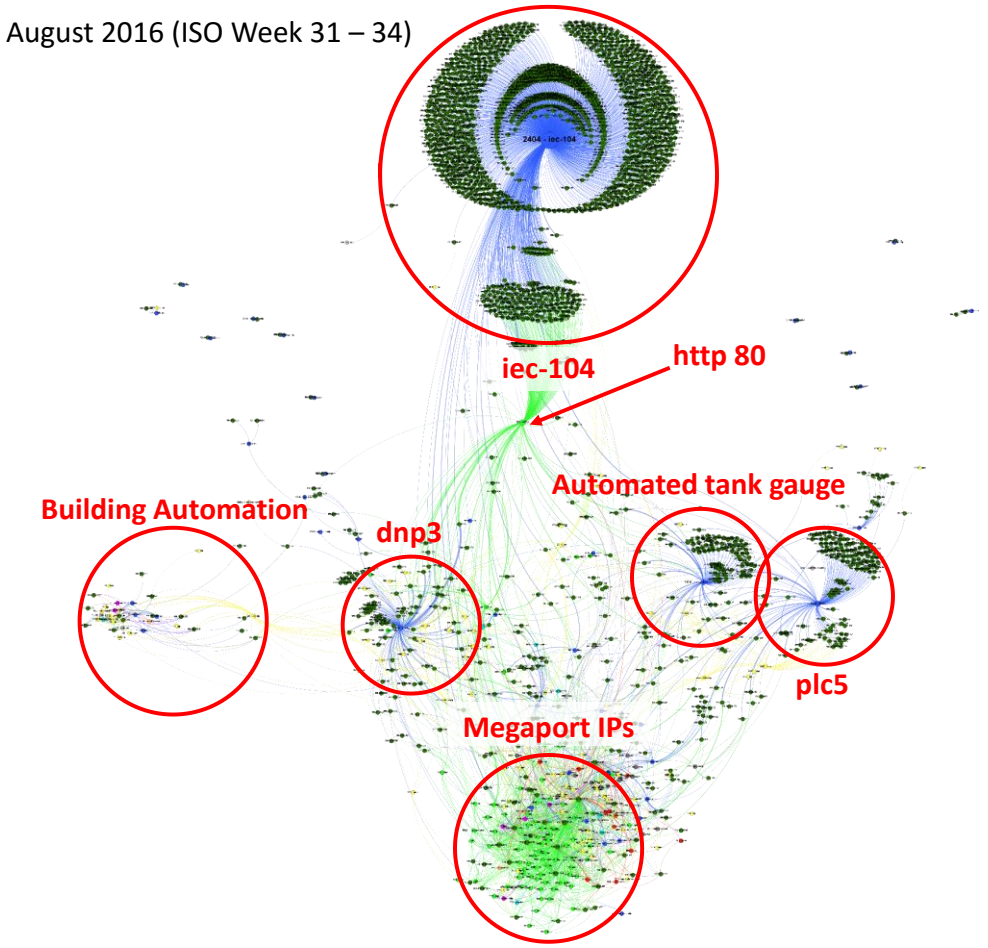

Figure 2: August 2016 ICS Network by Class

This visualization is the result of the Venezuela data from August 2016 and is based off what is essentially the shodanModules but referred to as “type”.

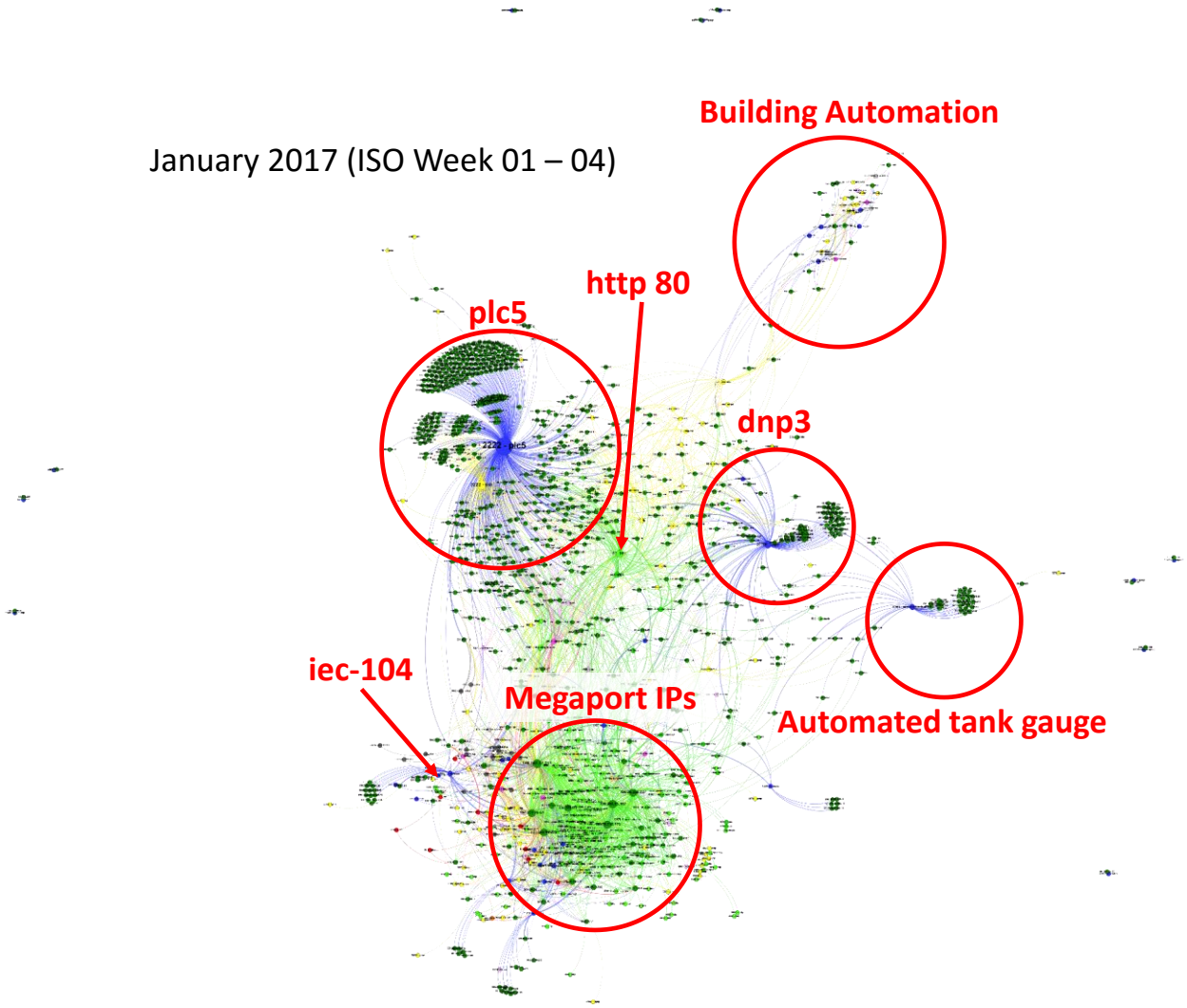

Figure 3: January 2017ICS Network by Class

This visualization is the result of the Venezuela data from January 2017 and was derived the same way as the August 2016 visualization.

Summary Statistics

Summary Statistics		
	August 2016	January 2017
IP Address Count	1912	730
Port/Module Count	264	337

Table 3: Summary Statistics of IPs and Ports

The visualizations created for both timeframes distributed the data (based off Force Atlas) into seven distinct areas of interest. In order to better understand what these areas are, the descriptions of the shodanModules were derived from the University of Arizona's database containing the parsed Shodan scans and information. Below you can find the following descriptions:

- ***iec-104***: one of the IEC 60870A set of standards which define systems used for telecontrol (supervisory control and data acquisition) in electrical engineering power system automation applications.

- ***http:*** data communication protocol for the internet

- ***plc5:*** Rockwell Automation Control System to the ControlLogix Control System. Customers are encouraged to migrate away from PLC-5

- ***automated tank guage:*** used to monitor fuel tank inventory levels, track deliveries, raise alarms that indicate problems with the tank or gauge (such as fuel spill), and to perform leak tests in accordance with environmental regulatory compliance. ATGs are used by nearly ever fueling station in the United States and tens of thousands of systems internationally.

- ***dnp3:*** DNP3 (Distributed Network Protocol) is a set of communication protocols used between components in process automation systems. Its main use is in utilities such as electric and water companies.

- ***Building Automation:*** The protocols being used within this region varied but all had to do with communication across building automation infrastructure or what appeared to be devices that facilitate the automation. Most of the protocols were unfamiliar.

- ***Megaport IPs:*** This region within the visualization contained the most amount of varied ports being open and was too dense to try and describe all of the port-protocol relationships. Many different protocols existed within this area and this could be due to devices residing behind a firewall or router. One interesting piece of discovery within this region was that certain IP addresses were connected to known malware shodanModules and that more than one piece of malware or malicious content was visible.

From the visualizations created based on the type / shodanModule class, it is apparent there are obvious differences. It can clearly be seen that the entirety of the iec-104 module from the August 2016 data is completely absent from the January 2017 data. Additionally, Shodan seemed to scan an increased amount of plc5 devices when comparing August to January as the visualizations represent a grown amount of IP addresses connected to this module over the time span. A few other insights can be seen within the shrink in the amount of connections to http port 80, but an increase in the Megaport IP address connections and growth of that cluster. Building Automation, automated tank gauge, and dnp3 seemed to stay relatively close in size. Despite the decrease in IP addresses within Venezuela scanned in January, only 731 as compared to 1913 in August, it seems as if the visualization actually appears more condensed within the core components. This can be attributed due to the increase in ports from 264 to 337 as noted in the summary statistics table.

Label	Type	Port	shodanModule	Aug 2016	Jan 2017	Difference
2404 - iec-104	ICS	2404	iec-104	1415	6	**-1409**
80 - http	HTTP	80	http	222	107	**-115**
2222 - plc5	ICS	2222	plc5	155	466	**+311**
10001 - automated-tank-gauge	ICS	10001	automated-tank-gauge	112	103	**-9**
20000 - dnp3	ICS	20000	dnp3	95	45	**-50**

Table 4: Notable Scan Differences

4.1.2 Modularity Visualizations

Modularity is a clustering algorithm in Gephi that can be used to identify neighborhoods in a graph. The number of neighborhoods found correlated to the settings used in running modularity.

Side by side comparison of August 2016 visualizations by modularity

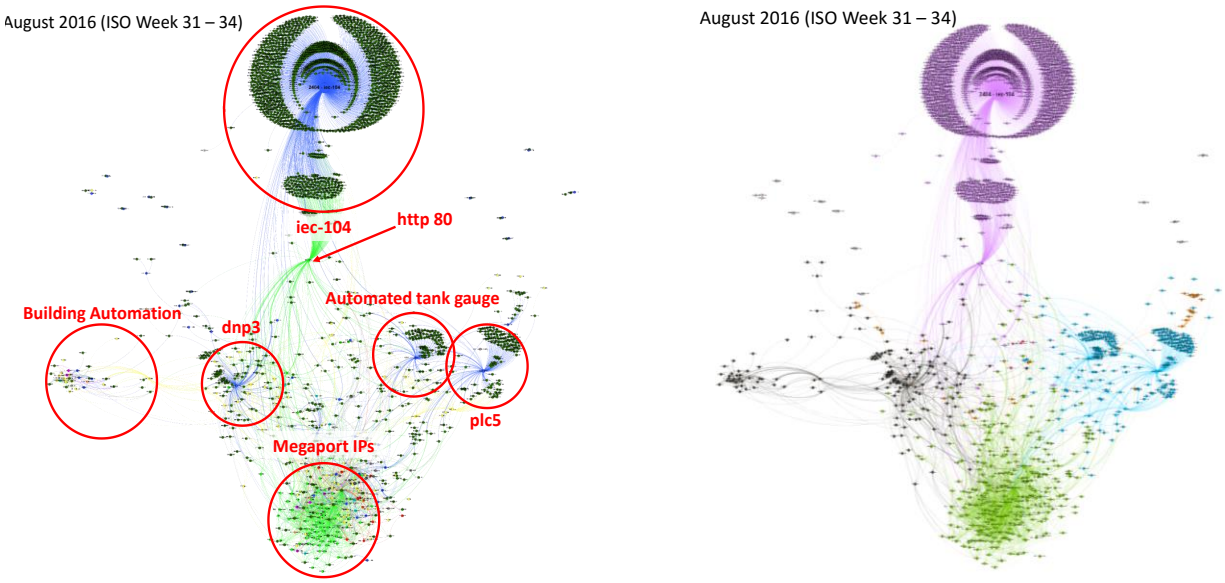

Figure 4: Comparison of August 2016 Visualizations

With the same dataset of IP nodes and port nodes, we chose to run a modularity based visualization as seen above in Figure 4. This visualization was created to gain insight on whether our data would create the same amount of neighborhoods as we defined within our type visualization. The difference here is that in the type visualization we defined and segregated the different port to IP relationships ourselves, whereas in modularity Gephi defines the groups based solely on the data. As seen above in the comparison, the neighborhoods created actually line up quite well with the ICS module that was used to scan. A few minor differences can be seen in that we do in fact have fewer neighborhoods (color representation) than we had originally self-identified. This can be

attested to the setting we used when created the modularity where it placed *automated tank guage* and *plc5* into the same class as well as *dnp3* and *building automation* modules.

Side by side comparison of January 2017 visualizations by modularity

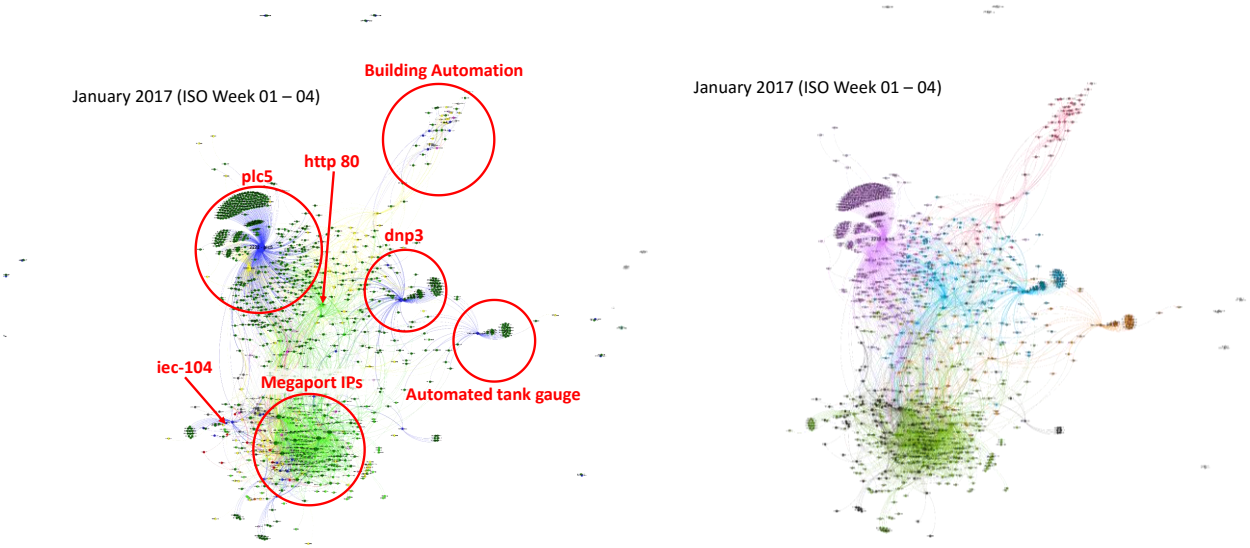

Figure 5: Comparison of January 2017 Visualizations

Here the correlation between modularity and the neighborhoods is more pronounced. As can be seen by the coloration of the neighborhoods, modularity identifies the different Shodan module protocols and areas that were pointed out in the previous visualizations. As seen in the August comparison, January contains fewer neighborhoods as well mostly due to the settings used here for the modularity visualization. The consistency amongst the two comparisons reassures that the IP port relations found amongst the ICS/SCADA devices within Venezuela were accurately identified via shodanModule.

4.1.3 IPs with the most open ports

August 2016				
IP Address	**Organization**	**ISP**	**Open Ports**	**Modularity**
186.167.17.211	Corporacion Digitel C.A.	Corporacion Digit	135	
190.202.29.62	CANTV	CANTV	101	
190.202.128.106	CANTV	CANTV	85	
104.224.0.3	Roya Hosting LLC	Roya Hosting LLC	81	
190.74.144.90	CANTV	CANTV	81	
200.84.151.86	CANTV	CANTV	75	
186.89.75.145	CANTV	CANTV	72	
200.84.249.231	CANTV	CANTV	60	
200.11.214.54	CANTV	CANTV	56	
172.111.133.3	Micfo, LLC.	Secure Internet LL	40	

January 2017				
IP Address	**Organization**	**ISP**	**Open Ports**	**Modularity**
186.167.17.211	Corporacion Digitel C.A.	Corporacion Digit	148	
190.202.25.182	CANTV	CANTV	132	
186.95.208.227	CANTV	CANTV	120	
190.79.215.223	CANTV	CANTV	118	
190.202.45.202	CANTV	CANTV	116	
190.202.29.62	CANTV	CANTV	114	
104.224.0.3	Roya Hosting LLC	Roya Hosting LLC	89	
186.95.80.51	CANTV	CANTV	68	
172.111.133.3	Micfo, LLC.	Secure Internet LL	59	
200.82.182.98	Internet Cable Plus, Mar	Internet Cable Plu	44	

Table 5: Top 10 IP Addresses per Time Period

Another interesting discovery here comes from considering the top 10 IP addresses for the respective time periods. The key thing to note here is the fact that only 4 IP addresses appear in both data sets (.211, .62, 133.3, 0.3). The state-owned incumbent CANTV is the country's exclusive provider of broadband based on DSL Networks ("Venezuela - Broadband And Digital Media Market - Statistics And Analyses - Buddecomm"). The importance here lies in knowing that they also potentially have the most exposed devices from an ICS/SCADA standpoint as they are the majority holder of the IP addresses we were able to analyze. Further research may need to

be conducted on what the other devices are to better understand why they have different ISPs. There may be some significance knowing that within these 4 IP addresses 3 of which are not owned by CANTV. Additionally, the two tables stay consistent with representing the shodanModule that they were attached to mostly *http* or *https* modules apart from the 3 IP addresses who had *test* as their shodanModule. The last noteworthy item is the overall majority increase in open ports discovered in January as opposed to August for these top 10 lists. This item relates back to Shodan because it is unknown if the tool actually scanned more ports on different IPs within January or if more ports actually became open and were therefore scanned and included within the data.

August 2016				
Shodan Module	**Port**	**Class**	**IP Addresses**	**Modularity**
iec-104	2404	ICS	1415	
http	80	HTTP	222	
plc5	2222	ICS	155	
automated-tank-gauge	10001	ICS	112	
dnp3	20000	ICS	95	
ssh	2222	Port	41	
https	443	HTTPS	36	
http	8080	HTTP	26	
rtsp-tcp	8554	Port	26	
ssh	22	Port	25	

January 2017				
Shodan Module	**Port**	**Class**	**IP Addresses**	**Modularity**
plc5	2222	ICS	466	
ssh	2222	Port	173	
http	80	HTTP	107	
dnp3	20000	ICS	103	
https	443	HTTPS	49	
http-simple-new	8080	HTTP	46	
automated-tank-gauge	10001	ICS	45	
ssh	22	Port	45	
ikettle	2000	IOT	42	
rdp	3389	REMOTE	37	

Table 6: Top 10 Port / Shodan Modules per Time Period

Due to this initial inconsistency within the Shodan data amongst the IP addresses scanned, it was important to also look at the top 10 port / shodanModules derived from our visualization. From Table 6, the first and foremost item of notice is the complete disappearance of the module *iec-104* in the January data. Once again this falls back onto Shodan and whether or not Matherly has decided not to scan for that port in January or that he completely ignored it as the landscape in Venezuela changed or that Shodan has some inconsistencies within its scanning techniques. Another drastic change in numbers amongst port and IP relationships is with *plc5*. This module increased almost exactly 3x as much from August to January. With this finding, we again question

Shodan's scanning techniques. It is unlikely that the country of Venezuela spawned close to 300 more devices all running *plc5* over the 5 month span, but rather Shodan may have scanned more intensely for *plc5* in January as the topic of the vulnerabilities around that module may have increased.

4.1.4 Key Findings Recap

This section briefly summarizes some major findings from the results discussed.

- 1,182 IP addresses were not scanned in January 2017
- 73 more ports were found open
- shodanModule *iec-104* was essentially eliminated from January 2017 scans
- shodanModule *plc5* grew three times as much from August to January
- Majority of IP addresses from both months belonged to government owned ISP CANTV

4.1.5 Future Research

From these findings, it can be determined that inconsistencies do exist within Shodan data for a small scaled dataset. Further research efforts could be conducted to better understand why Shodan scans differ so much, or if this specific study was an anomaly due to its size. Another area for research would be to understand what types of devices exist within Venezuela beyond just the port and IP relationships used within this study. Expansion of the dataset to include potentially all of the countries within Latin America could help provide further proof that data collection and scanning may need to be own on an as-need basis by the researchers or that Venezuela was a standout from the norm for Shodan.

5 CONCLUSION

In conclusion, representing the ICS/SCADA devices found in Venezuela through visualizations allowed for accurate representation of the landscape for that country. However, through our data analysis some findings did show that scans varied over the 5-month span from August 2016 to January 2017. Shodan data may be very valuable from providing data on any device it can scan over the internet, however more work needs to be performed on analyzing if the scans stay consistent over a time period. Shodan should also still be evaluated on a larger scale for its accuracy and consistency in identifying open ports over the same IP range. Through the data analysis and visualizations, our case study did have success in analyzing Venezuela as well as provide insightful information for future research efforts.

REFERENCES

Attipoe, Antoinette E.; Yan, Jie; Turner, Claude; Richards, D. (2016). Visualization Tools for Network Security. *Electronic Imaging*, *Visualization*, 1–8.

Balakrishnan, Balaji (2015). Security Data Visualization. SANS Institute InfoSec Reading Room.

Bodenheim, R., Butts, J., Dunlap, S., & Mullins, B. (2014). Evaluation of the ability of the Shodan search engine to identify Internet-facing industrial control devices. *International Journal of Critical Infrastructure Protection*, 7(2), 114–123. http://doi.org/10.1016/j.ijcip.2014.03.001

Bodenheim, R. C. (2014). Impact of the Shodan Computer Search Engine on Internet-facing industrial control system devices.

Diniz, Gustavo, and Robert Muggah. "A fine balance: mapping cyber (in) security in Latin America." *Igarapé Institute and SecDev Foundation-Strategic Paper* 2 (2012).

E. Ayuburi and L. Sobrevinas, “Securing Supervisory Control and Data Acquisition Systems: Factors and Research Direction,” in Americas’ Conference on Information Systems (AMCIS), 2015.

Ercolani, V. J., Patton, M. W., & Chen, H. (2016, September). Shodan visualized. In *Intelligence and Security Informatics (ISI), 2016 IEEE Conference on* (pp. 193-195). IEEE.

Genge, Béla, and Călin Enăchescu. "ShoVAT: Shodan- based vulnerability assessment tool for Internet- facing services." *Security and communication networks* (2015).

Glickhouse, Rachel. "Explainer: Fighting Cybercrime In Latin America". *AS/COA*. N.p., 2013. Web. 5 May 2017. http://www.as-coa.org/articles/explainer-fighting-cybercrime-latin-america

I. Onyeji, M. Brazilian, and C. Bronk, "Cyber Security and Critical Energy Infrastructure," Electr. J, vol 27, no. 2, pp. 52-60, Mar 2014.

"Latin America Reaches A Crossroads For Guarding Against Cybercrime - Knowledge@Wharton". *Knowledge@Wharton*. N.p., 2013. Web. 5 May 2017. http://knowledge.wharton.upenn.edu/article/latin-america-reaches-a-crossroads-for-guarding-against-cybercrime/

Mattern, Benjamin. "Cyber Security And Hacktivism In Latin America: Past And Future". *Coha.org*. N.p., 2017. Web. 5 May 2017. http://www.coha.org/cyber-security-and-hacktivism-in-latin-america-past-and-future/

Micro, Trend. "Latin American and Caribbean Cybersecurity Trends and Government Responses.",http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-tendencias-en-la-seguridad-cibernetica-en-america-latina-y-el-caribe-y-respuestas-de-los-gobiernos. Pdf, (2013). https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-latin-american-and-caribbean-cybersecurity-trends-and-government-responses.pdf

Samtani, Sagar, et al. "Identifying SCADA vulnerabilities using passive and active

vulnerability assessment techniques." *Intelligence and Security Informatics (ISI), 2016 IEEE Conference on*. IEEE, 2016. DOI: 10.1109/ISI.2016.7745438

http://ieeexplore.ieee.org.ezproxy2.library.arizona.edu/stamp/stamp.jsp?arnumber=7745438

"Venezuela - Broadband And Digital Media Market - Statistics And Analyses - Buddecomm". *Budde.com.au*. N.p., 2017. Web. 5 May 2017.