Scanning the Internet for Vulnerable Devices

Anna Sim
UT Austin

Sean Wang
UT Austin

ABSTRACT

We scan the internet for vulernable devices, focusing on select vulerabilities, using Shodan. Then, we analyze the data to see what the detected machines have in common. Additionally, we create our own scanner to scan the internet for machines vulernable to the same vulnerabilities and compare the results to those of Shodan's scan.

1. INTRODUCTION

With the growth and popularization of the intnert more and more devices are becoming connected to each other through the internet. This allows many devices to now have the convenience and accessibility of being connected to other devices through the internet, such as printing to a shared printer connected to the internet or controlling security cameras remotely.

However, a key problem that comes hand in hand with these advantages is that any any vulnerabilities could allow unwanted and unauthorized guests to control the device remotely. Devices without proper security can be attacked and the attackers can then control the devices and gain access to any information the device might have. In some cases, attackers can utilize the connection and control they have over the device to then attack the other devices connected to the same network. For example, Shodan is a tool that allows users to search for devices connected to the internet and can give potentially useful information for attackers. Currently, there are many computer systems, including traffic lights, security camers, or industrial control systems, that have little to no security, leaving them vulnerable to attackers[5].

The approach taken in this paper is to determine some Common Vulnerabilities and Exposures (CVEs) that can be detected remotely and then utilize Shodan to see how many machines have those vulnerabilities and what similarities the machines have. Then, since one approach to defense against this type of detection is to just prevent detection by Shodan, a custom scanning tool will be used to see if it has similar results.

Overall, the setup is simple and is mostly data analysis and comparison. The data returned by Shodan's search will be divided by the CVE that the machine is vulnerable to, but will also need to have the flexibility to pick a machine and see what CVEs Shodan determined it to be vulnerable to.

The methods for a custom scanner for specific CVEs will depend on the specific CVEs chosen. In this case, we plan to look at CVE-2014-2256, CVE-2019-0708, and CVE-2018-0101.

The main contributions of this paper are as follows:

- We explore more about the vulernabilities being searched for and provide more detail on how these can be exploited for some specific systems.

- We show how these vulernabilities can be detected using Shodan and what information can be gathered from these scans. We analyze this information and discuss how this could be used maliciously.

- We create our own scanner and compare its results to Shodan to get insight on how information of specific systems is exposed to the internet.

2. MOTIVATION

For this project, the works that we will build on most are the "Evaluation of the ability of the Shodan search engine to identify Internet-facing industrial control devices", "Impact of the Shodan Computer Search Engine on Internet-facing Industrial Control System Devices," and "Contactless Vulnerability Analysis using Google and Shodan."

All of the above mentioned works cover the Shodan search engine which will be helpful in starting this project and knowing what we can do to perform our own form of vulnerability analysis. The second report explains in more detail compared to the other two about the Shodan program itself, such as its functionality and device identification, indexing, as well as its setup and deployment. Together, these reports in addition to previous labs involving internet scanning will help us achieve our goal in discovering vulnerable machines found by our script.

The CVEs listed previously were chosen due to their commonality, since this would mean that there would be more information to work with. Additionally, that gives the custom scanner more opportunities in the situation that it does not perform as well as Shodan, so that a better comparison can be made between the two scanning methods.

3. OUR ARCHITECTURE

Since there are three different CVEs to look at, the methods used to scan for devices vulnerable to those will be slightly different, both with Shodan and our custom scanning tool.

For CVE-2014-2256, the vulnerability is described as an issue with Siemens SIMATIC S7-1200 CPU PLC devices that have an older firmware that allows remote attackers to execute a Denial of Service (DoS) attack[1]. On Shodan, the exact search term used to find these vulnerable devices is: `siemens port:"102"`. The DoS attack is caused by attackers sending ISO-TSAP, or TCP, packets to specifically port 102, since this port is left open by the firmware. Then, for the custom tool, we use `zmap` to scan on port 102 and get a list of devices probed, which could be longer than the list from Shodan, since there is no filtering for the specific vulnerable devices we are looking for. Then, we filter for devices by getting OS information from `nmap` to determine the final list of devices.

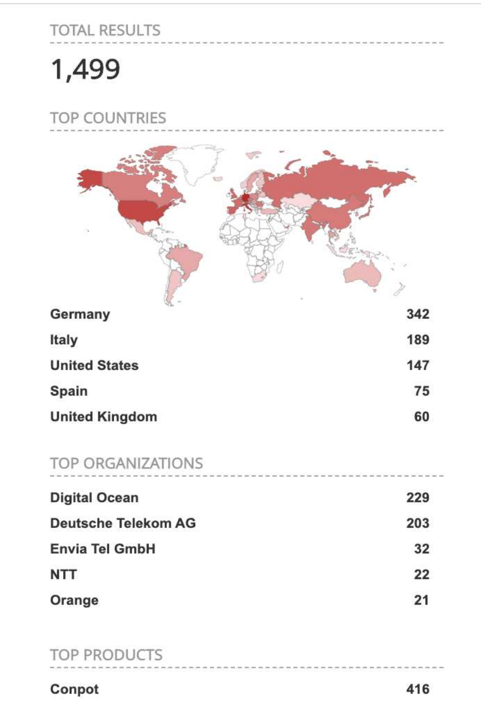
CVE-2019-0708 is described as a remote code execution vulnerability that exists in Microsoft's Remote Desktop Protocol in Windows[3]. In Shodan, we need several searches for devices with port 3389 open and running versions of Windows that could potentially be vulnerable. This means our searches combines the term `port:"3389"` with one of the following: `os:"Windows 7 or 8"`, `os:"Windows XP"`, `2003`, or `2008`. In this case, the last two terms refer to versions of Windows Server. Our custom tool utilizes `nmap` to detect for an open port 3389 as well as the OS. Then the results are filtered for the versions of Windows we are looking for.

Finally, CVE-2018-0101 is a vulnerability in Cisco's Adaptive Security Appliance (ASA) Software, specifically the Secure Sockets Layer (SSL) VPN functionality. This vulnerability could allow remote execution of a code and is possible since enabling the webvpn feature will cause an attempted double free on a region of memory on the device. This is detectable by checking to see if the Cisco ASA device has the webvpn feature enabled. The National Vulnerability Database provides a list of specific devices affected by this vulnerability[2]. In Shodan, we use the search term `"Set-Cookie: webvpn=;" ssl:"ASA Temporary"`, since the ASA Software sets a the webvpn cookie. Using just the webvpn filter may also capture other devices where some other web applications might have set the cookie as well, but the ASA Temporary SSL certificate filter gives a narrower set of search results of devices vulnerable to this CVE. Our custom tool to scan for this vulnerability is a honeypot that detects exploitation attempts by listening on port 443 and records the vulnerable IPs that it detects.

4. EXPERIMENTAL RESULTS

For CVE-2014-2256, the Shodan search using the term `siemens port:"102"` returned 1,499 results, with the top five countries the results are from being Germany, Italy, United States, Spain, and United Kingdom, as shown in Figure 1. Our custom tool, on the other hand, discovered 801 internet facing devices on port 102 after a zmap scan of 10000 seconds.

For CVE-2019-0708, the Shodan search for `port:"3389"` returned 5,095,829 results, but would need to be narrowed down based on the operating system. Adding the term `os:"Windows 7 or 8"` to the original search term returned 12,012 results, shown in Figure 2. Adding `os:"Windows XP"` to the original search term returned 1,957 results. Adding `2003` to the original search term returned 32,560 results. Adding `2008` to the original search term returned 32,802 results. Our custom scanning script discovered 2354 internet facing devices on port 3389 after scanning for 10000 seconds.



TOTAL RESULTS

1,499

TOP COUNTRIES

Germany	342
Italy	189
United States	147
Spain	75
United Kingdom	60

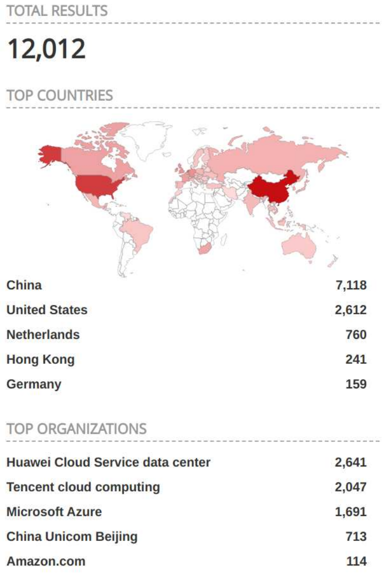
TOP ORGANIZATIONS

Digital Ocean	229
Deutsche Telekom AG	203
Envia Tel GmbH	32
NTT	22
Orange	21

TOP PRODUCTS

Conpot	416

Figure 1: Shodan search results for CVE-2014-2256



TOTAL RESULTS

12,012

TOP COUNTRIES

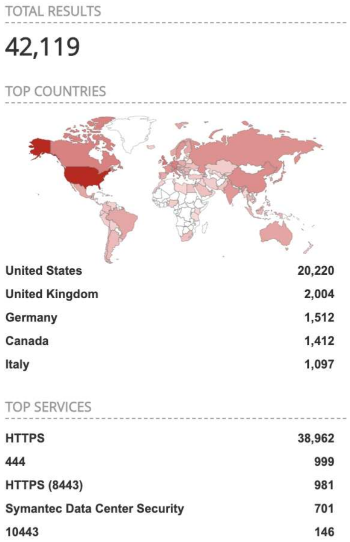
China	7,118
United States	2,612
Netherlands	760
Hong Kong	241
Germany	159

TOP ORGANIZATIONS

Huawei Cloud Service data center	2,641
Tencent cloud computing	2,047
Microsoft Azure	1,691
China Unicom Beijing	713
Amazon.com	114

Figure 2: Shodan search results for CVE-2019-0708, where the device OS is Windows 7 or 8

Finally, for CVE-2018-0101, the Shodan search for `"Set-Cookie: webvpn=;" ssl:"ASA Temporary"` returned 42,119 results. The top five countries these results were from are United States, United Kingdom, Germany, Canada, and Italy, with the exact numbers shown in Figure 3.



TOTAL RESULTS

42,119

TOP COUNTRIES

United States	20,220
United Kingdom	2,004
Germany	1,512
Canada	1,412
Italy	1,097

TOP SERVICES

HTTPS	38,962
444	999
HTTPS (8443)	981
Symantec Data Center Security	701
10443	146

Figure 3: Shodan search results for CVE-2018-0101

5. RELATED WORK

In ”Impact of the Shodan Computer Search Engine on Internet-facing Industrial Control System Devices”[5], they discuss metrics on whether or not Shodan has been and is being used to target industrial control system devices. This addresses the concern of whether this method and channel of attack are widely used when targetting a specific set of devices.

In another paper, ”Evaluation of the ability of the Shodan search engine to identify Internet-facing industrial control devices”[4], they analyze Shodan’s detection ability on a specific programmable logic controller and suggests a potential solution to mitigate its visibility to Shodan.

In ”Shodan Visualized”[6], the paper discusses how Shodan actually scans the internet. Shodan works by scanning the internet for open ports on IP addresses and determines runnings services on chosen ports. In order to visualize these open ports, they create visualizations that use both IP addresses and open ports as nodes. The team focuses on identifying Supervisory Control and Data Acquisition (SCADA) and Industrial Control System (ICS) devices due to the infrastructural support of these devices. Shodan visualizations can provide a solution in understanding what devices are running on a network.

In ”Contactless Vulnerability Analysis using Google and Shodan”[7], the paper discusses combining Google searches and Shodan searches to determine the vulnerability of systems in large scale networks. This contactless vulnerability analysis suggests a potential solution in analyzing vulnerable domains by refining search terms and combining results from Google and Shodan.

6. CONCLUSIONS

We expect that Shodan can detect these vulnerabilities and that not all machines with these vulnerabilities have been patched, since it may be harder to patch on certain machines than others. Additionally, we expect that the results of our own scanner to be similar to Shodan’s scan, but with less results.

7. REFERENCES

[1] Cve-2014-2256 detail, March 2014.

[2] Cve-2018-0101 detail, October 2019.

[3] Cve-2019-0708 detail, July 2019.

[4] R. Bodenheim, J. Butts, S. Dunlap, and B. Mullins. Evaluation of the ability of the shodan search engine to identify internet-facing industrial control devices. Technical report, Air Force Institute of Technology, Jan. 2014.

[5] R. C. Bodenheim. Impact of the shodan computer search engine on internet-facing industrial control system devices. Technical report, Air Force Institute of Technology, Mar. 2014.

[6] V. J. Ercolani, M. W. Patton, and H. Chen. Shodan visualized. 2016.

[7] K. Simon, C. Moucha, and J. Keller. Contactless vulnerability analysis using google and shodan. 2017.