Reducing The Threat Foot Print By Enemy Emulation

01 Introduction

Continuous integration, development, and deployment have given rise to an interesting habit in which many organizations now stand up and tear down infrastructure at an alarming rate. A system can erupt into existence and then vanish just as quickly. Scanning of network infrastructure is invaluable and the tool Shodan can function as an excellent supporting technology.

02 The Problem

Computer systems across the internet are being deployed without an acceptable end of life management scheme. They are not receiving updates and they are not being monitored by their owners. This has led to a host of problems, including numerous systems being left exposed to very dangerous exploits and not being updated as necessary. The lack of attention to detail means we are continuing to see issues related to Log4J, Outlook, and other major exploits available over the internet even today.

03 Project Scope, Goals, and Objectives

The goal of this project is to assist in the safety and security of the United States by hunting for systems that are currently functioning as a beacon online and that have not received updates when they should have been. Students will not be performing active scanning but will instead use Shodan to gather their data and sift for vulnerable systems. Any system that is made publicly available by Shodan will be considered within the scope of this project.

04 Solution and Action Plan

Students have deployed a Shodan student account to scan systems on the internet and look for flaws. Many of our students are using the Shodan command line interface to search for systems that have not been updated or are currently vulnerable to a plethora of systems. After conducting their search, they provide that information to their instructor, and then the instructor will triage the data and make a decision on who to send the information to.

05 Risk Management Analysis

All data gathered by the students is open source and publicly available. No connection to any system will be made and no verification of the data will be made beyond what is provided by Shodan. Students will not be communicating with any parties involved and all data will be managed through a strict chain of command. There is very little risk to the educational institution or the students and any data gathered can be provided as a link from the Shodan web application.

06 Anticipated Project Results

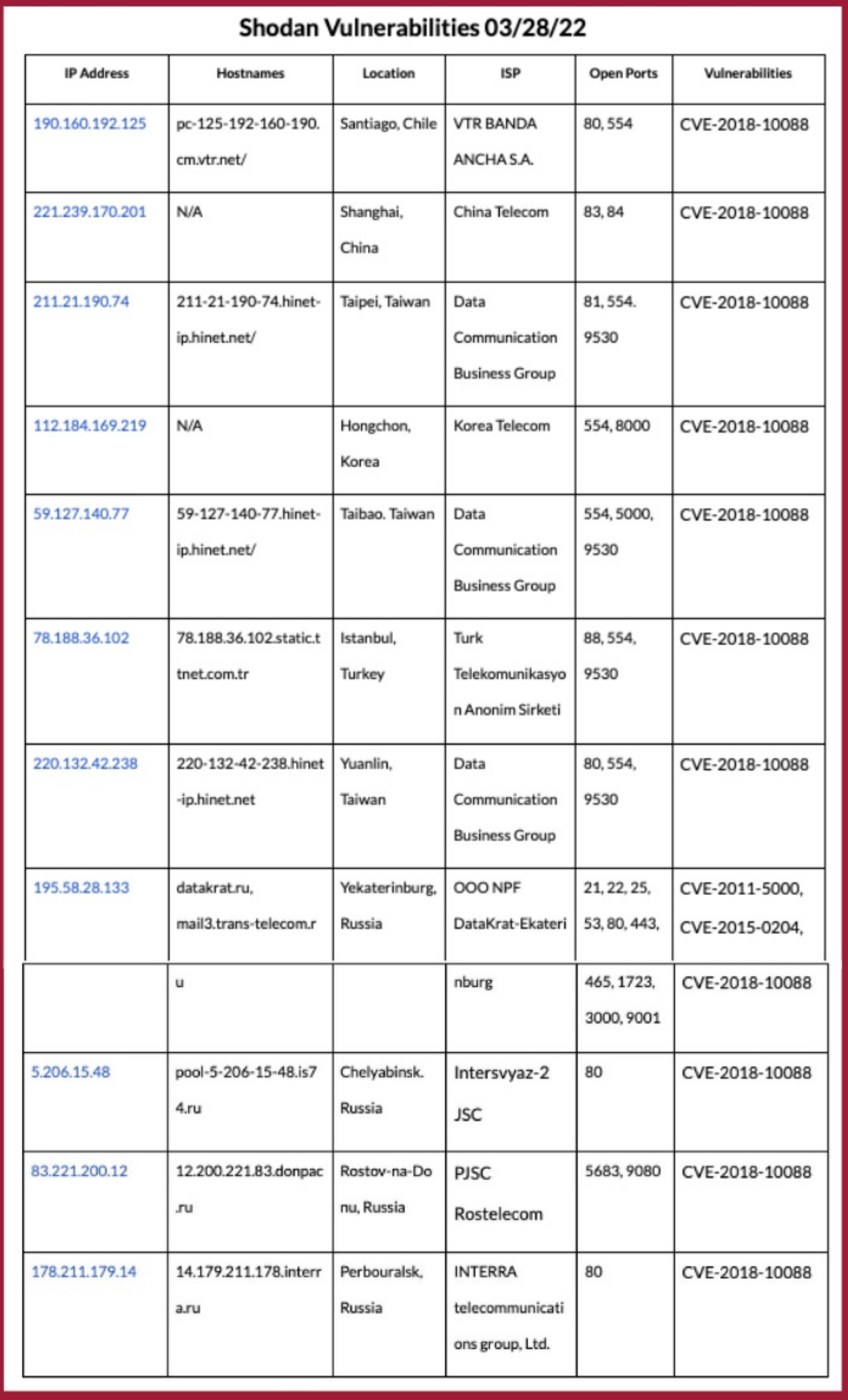
We anticipated that this project would spark interest in the security of systems across the nation. Students were expected to find vulnerable systems and report them so that they could be pushed up the chain of command. This project was expected to gain interest from numerous sectors within the State of Arizona and it has done so.

07 Proposed Costs

Free. Shodan will graciously provide a student account to any student with an EDU email. Students work on this project during their production studio and no costs are incurred by the organization or any benefactors of the project.

08 Conclusion

Faculty have received phone calls from law enforcement and cyber parties across the nation in reference to data provided. Students have discovered open camera systems, vulnerable critical infrastructure, and systems related to the nuclear power industry. This information was properly curated and pushed to the appropriate authorities. This project has been on-going for more than a year and has cost nothing. We have seen a tremendous interest in this project from local authorities and have fielded phone calls and online meetings with parties interested in our results.



Shodan Vulnerabilities 03/28/22

IP Address	Hostnames	Location	ISP	Open Ports	Vulnerabilities
190.160.192.125	pc-125-192-160-190.cm.vtr.net/	Santiago, Chile	VTR BANDA ANCHA S.A.	80, 554	CVE-2018-10088
221.239.170.201	N/A	Shanghai, China	China Telecom	83, 84	CVE-2018-10088
211.21.190.74	211-21-190-74.hinet-ip.hinet.net/	Taipei, Taiwan	Data Communication Business Group	81, 554. 9530	CVE-2018-10088
112.184.169.219	N/A	Hongchon, Korea	Korea Telecom	554, 8000	CVE-2018-10088
59.127.140.77	59-127-140-77.hinet-ip.hinet.net/	Taibao. Taiwan	Data Communication Business Group	554, 5000, 9530	CVE-2018-10088
78.188.36.102	78.188.36.102.static.ttnet.com.tr	Istanbul, Turkey	Turk Telekomunikasyon Anonim Sirketi	88, 554, 9530	CVE-2018-10088
220.132.42.238	220-132-42-238.hinet-ip.hinet.net	Yuanlin, Taiwan	Data Communication Business Group	80, 554, 9530	CVE-2018-10088
195.58.28.133	datakrat.ru, mail3.trans-telecom.ru	Yekaterinburg, Russia	OOO NPF DataKrat-Ekaterinburg	21, 22, 25, 53, 80, 443, 465, 1723, 3000, 9001	CVE-2011-5000, CVE-2015-0204, CVE-2018-10088
5.206.15.48	pool-5-206-15-48.is74.ru	Chelyabinsk. Russia	Intersvyaz-2 JSC	80	CVE-2018-10088
83.221.200.12	12.200.221.83.donpac.ru	Rostov-na-Donu, Russia	PJSC Rostelecom	5683, 9080	CVE-2018-10088
178.211.179.14	14.179.211.178.interra.ru	Perbouralsk, Russia	INTERRA telecommunications group, Ltd.	80	CVE-2018-10088