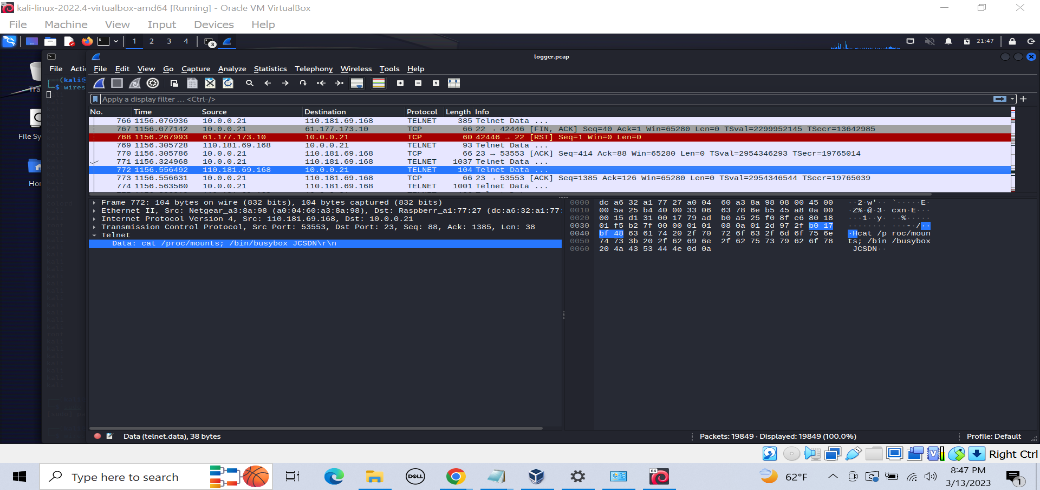
The Hajime botnet malware can be run to SYN scan the internet and discover open TCP/23 (telnet) and TCP/5358 (WSDAPI) ports. Hajime brute forces these open sockets with a list of 63 credentials, "61 factory default passwords from Mirai and adds 2 new entries ‘root/5up’ and ‘Admin/5up’ which are factory defaults for Atheros wireless routers and access points" - https://www.infopoint-security.de/media/Botnet\_Hajime\_Radware\_Analyse.pdf. If an instance connects successfully and gets a shell, the Hajime malware will immediately look for a place to drop malware into by issuing `cat /proc/mounts; /bin/busybox RANDOM\_TAG` and will also check to see if programs like curl and wget are installed. The purpose for the busybox command is to indicate that the command is completed. " A trick used by many malwares is to use a non-existent busybox applet to signal the completion of every command issued." - https://0x00sec.org/t/iot-malware-droppers-mirai-and-hajime/1966/1.



Once an appropriate partition is selected and changed into, Hajime will attempt to discover the architecture of the system in order to download the right malware. It will do this by copying a binary (typically /bin/echo) into the current working directory and cat out the contents.

A screenshot of a computer

Description automatically generated

The attacker does this by issuing the commands "dd bs=52 count=1 if=.s || cat .s || while read i; do echo $i; done < .s\r\n".

A screenshot of a computer

Description automatically generated

The telnet session will succeed in printing the contents for .s twice and then fail on the third command.

A screenshot of a computer

Description automatically generated

I noticed after this, the attacking malware exits the shell and the connection ends.

A screenshot of a computer

Description automatically generated

I found it to be peculiar that the second and third command executed even after the first command succeeded(after a double pipe). I assume the malware did as well and found it to be indicitive of a honeypot and stopped.